

DMM Working Group  
Internet-Draft  
Intended status: Informational  
Expires: January 12, 2014

H. Ali-Ahmad (Ed.)  
Orange  
D. Moses  
H. Moustafa  
Intel Corporation  
P. Seite  
Orange  
T. Condexia  
University of Aveiro  
July 11, 2013

Mobility Anchor Selection in DMM: Use-case Scenarios  
draft-aliahmad-dmm-anchor-selection-01.txt

Abstract

This document presents and discusses different use-case scenarios of mobility anchor selection in Distributed Mobility Management (DMM).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 12, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Terminology . . . . .	3
2. Introduction . . . . .	4
3. Considered contexts . . . . .	5
3.1. Mobile node context . . . . .	5
3.2. Application context . . . . .	6
3.3. Network context . . . . .	8
4. Use-case scenarios . . . . .	9
4.1. Extremely mobile nodes without any typical location . . . . .	9
4.2. Mobile nodes with one or more typical locations . . . . .	10
4.3. Fairly stationary nodes . . . . .	12
5. Security Considerations . . . . .	13
6. IANA Considerations . . . . .	14
7. Acknowledgements . . . . .	15
8. References . . . . .	16
8.1. Normative References . . . . .	16
8.2. Informative References . . . . .	16
Authors' Addresses . . . . .	17

## 1. Terminology

### IP-handover:

a handover of a mobile node at the IP level resulting in an IP address change at the mobile node.

### New flow:

a flow that did not undergo any IP-handover.

### Handover flow:

a flow that did undergo one or more IP-handovers.

### New traffic:

the data traffic of the new flows.

### Handover traffic:

the data traffic of the handover flows.

### Current access router:

the access router where the mobile node is currently attached at the IP level.

### DMM default mode of mobility anchor selection:

new flows are always anchored at the current access router which acts as the mobility anchor for these flows after an IP-handover.

## 2. Introduction

Distributed Mobility Management (DMM) aims at overcoming the shortcomings of the existing IP mobility protocols, such as Mobile IPv6 [RFC6275] and Proxy Mobile IPv6 [RFC5213], that are considered centralized. It brings the mobility anchor closer to the mobile node, down at the access routers level. This is the enabler of a concept that is so-called dynamic mobility, where the mobile node changes its mobility anchor for new flows. New flows are always initiated using the mobile node's current IP address which is configured using the prefix provided by the current access router. The data traffic of these flows is then routed optimally until the mobile node undergoes an IP-handover. However, upon an IP-handover, tunneling mechanisms are needed with that access router, which is then considered the mobility anchor of those flows initiated using its prefix during the whole lifetime of those flows. In what follows, this is considered the DMM default mode of mobility anchor selection.

If most of the flows are short enough to not undergo one or more IP-handovers, it is expected that most of the data traffic is routed optimally. However, this assumption is not always valid and the mobility anchor for new flows, when initiated, could be selected in a more appropriate manner.

When a flow is initiated, it is assigned a mobility anchor that lasts during its whole lifetime. Thus, selecting the most appropriate mobility anchor for a flow when initiated can significantly enhance the mobility management performance, e.g. less overhead, shorter end-to-end delay. Thus, a DMM solution should allow selecting and using the most appropriate mobility anchor among a set of distributed ones [I-D.ietf-dmm-best-practices-gap-analysis]. In order to achieve this, different metrics and contexts should be taken into consideration. Distributing the mobility anchor functionalities at the access routers level allows considering several contexts such as the mobile node's mobility context, the application context, and the network context.

Hereafter in this document, the considered contexts are presented and then the different use-case scenarios are discussed.

### 3. Considered contexts

#### 3.1. Mobile node context

The mobile node's mobility has an important effect on the mobility anchor selection. For example, a mobile node with high mobility undergoes frequent IP-handovers. When considering DMM default mode of mobility anchor selection, almost all the traffic of such mobile node is handover traffic, moreover, the number of simultaneous anchors and tunnels may increase. On the other hand, flows of mobile nodes with low mobility are more likely to be initiated and terminated before undergoing an IP-handover.

In addition, the mobile node's location with respect to the different mobility anchors influences selecting one of them for new flows. For example, locating the mobility anchor as close as possible to the mobile node results in a shorter tunnel, and hence less tunneling overhead, when tunneling mechanisms are required. The most appropriate mobility anchor is the closest one to the mobile node during the longer portion of the flow lifetime. At the instant of initiating a new flow, the current access router is the closest one to the mobile node. However, the mobile node may undergo an IP-handover and attach to another access router. Whether the longer portion of the flow is before or after the IP-handover has an effect on selecting the most appropriate mobility anchor for this flow.

Moreover, a mobile node may have one or more "typical locations" where it attaches to the network most of the time, e.g. at home. This helps expecting the mobile node's location for relatively long durations and, consequently, in selecting the most appropriate mobility anchor by using information about typical location(s). Note that some statistics show that users spend more than 60% of their time at home and work [Cisco-VNI].

Finally, the mobile node's attachments history is needed in order to take into consideration the mobile node's mobility and location as described above.

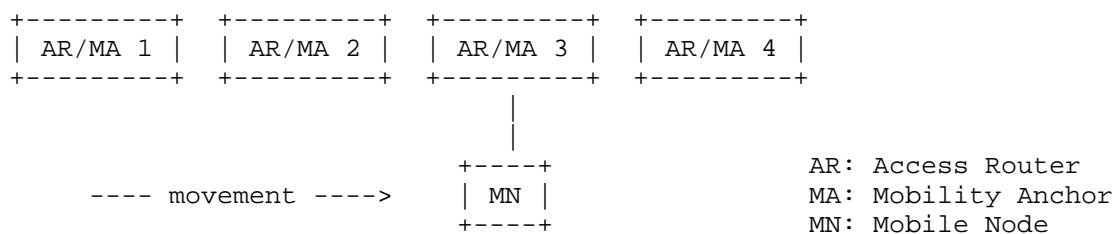


Figure 1: Mobile node's movement in DMM network

### 3.2. Application context

Based on the application, the need of IP continuity and the flow characteristics can be estimated. While applications that require IP continuity cause the establishment of tunnels in the access network upon an IP-handover, applications that can tolerate an IP address change at the application layer, e.g. SIP-based sessions, do not [I-D.ietf-dmm-requirements]. The mobility anchor selection is less important in the latter case due to the capability of changing the IP address. In fact, there is no need for tunneling and hence no need for a mobility anchor since the application can tolerate any change in the IP address; hence, all the traffic is routed using standard routing schemes.

In addition, the flow characteristics are highly dependent on the application. Some applications generate in general long flows such as multimedia (e.g. video streaming), online gaming, large files downloading, etc. (see Table 1 below); others generate in general short flows such as TCP connections for HTTP and SMTP sessions. Long flows are more likely to undergo one or more IP-handovers and therefore the mobility anchor selection can play an important role to enhance the mobility management performance. On the other hand, short flows are more likely to be initiated and terminated before an IP-handover.

In the following table, we present some examples on different types of applications. For each application, we mention the expected (or probable) traffic and mobility characteristics as well as the possible types of devices used for such application. The objective of this list of applications is to show later some possible real mapping(s) for the different use-case scenarios.

Application	Traffic Type	Mobility Nature	User Device	Comments
RT Gaming	Long flows with IP continuity req	Stationary or mobile (depending on game)	Laptop, tablet, smartphone, game console	For game consoles, the device and traffic characteristics could be easily predicted
Audio/Video conferencing	Long flows with IP continuity req	Stationary or mobile	Smartphone, tablet, laptop	
Live streaming IPTV	Long flows with IP continuity req	Stationary or mobile	Large screen TV, laptop, tablet, smartphone	If a large screen TV, client is stationary. Otherwise, client is mobile
Waze	Long flows without IP continuity req	Mobile	Smartphone, dedicated car GPS (future)	A typical location (Ski resort)
GoPro	Long flows with IP continuity req	Mobile	GoPro camera	
Video Report	Long flows with IP continuity req	Stationary or mobile	Mobile surveillance, HD camera	

Video streaming in vehicles	Long flows with IP continuity req	Mobile	Car TV, tablet, smartphone	If the car is mainly used in specific neighborhood a typical location is irrelevant
Camcorder download	Long flows with IP continuity req	Stationary or mobile	Camcorder	
HTTP and SMTP sessions	Short flows with IP continuity req	Stationary or mobile	Smartphone, tablet, laptop	

Table 1

### 3.3. Network context

When a mobility anchor is assigned to a flow (when the flow is initiated), it acts as a mobility anchor for this flow the whole flow's lifetime. It is responsible to forward the flow's data packets if the mobile node is physically attached to it. It is responsible, in addition, to encapsulate and de-capsulate the flow's data packets if the mobile node is not attached to it and tunneling mechanisms are used.

Even with distributed mobility anchors, the distribution of the active mobile nodes in the network is not necessarily even. As a result, some mobility anchors are overloaded more than others. It is then reasonable to take into consideration the estimated (or projected) level of load of the mobility anchors as well as the access network characteristics/resources when selecting one of them for a new flow (the metrics for measuring this level are left for specific implementations).



#### 4. Use-case scenarios

##### 4.1. Extremely mobile nodes without any typical location

Extreme mobility could be due to either a high mobile node's speed, or a small access router's coverage area, or both.

###### Scenario 1: running applications generating typically short flows

Short flows are more likely to be initiated and terminated before the mobile node undergoes an IP-handover. Even if a flow experiences an IP-handover, it is expected that the flow does not last long after the IP-handover. In other words, most of the mobile node's traffic is new traffic in this scenario. As a result, the closest mobility anchor to the mobile node during the longest portion of a flow is its current access router. It is recommended then to always anchor new flows at the current access router, which is the DMM default mode of mobility anchor selection.

A well known example on short flows is the TCP connections for HTTP and SMTP sessions.

###### Scenario 2: running applications generating typically long flows

For extremely mobile nodes, it is more likely that a flow experiences an IP-handover soon after being initiated. And since the flows are long-lived, it is expected that a flow lasts for a long duration after the IP-handover(s). As a result, it could be said that most of the traffic is handover traffic in this scenario. Whatever is the mobility anchor selection criterion, most of (almost all) the mobile node's data traffic needs tunneling mechanisms. Thus, the mobility anchor selection cannot play a significant role regarding the route optimization or the tunneling overhead reduction.

However, there are number of consequences regarding the control plane e.g. number of simultaneous anchors/tunnels for a mobile node and the related contexts and signaling loads. First, let us consider the DMM default mode of mobility anchor selection. Since new flows are always anchored at the current access router, each flow initiated between two consecutive IP-handovers is anchored at a different mobility anchor. With extremely mobile node, long flows are expected to experience several IP-handovers and their mobility anchors are expected to be maintained for a long duration. As a result, the number of simultaneous anchors/tunnels for a mobile node may increase as well as the related contexts and

signaling loads. This affects the control plane negatively.

As the DMM default mode does not achieve data plane optimization in the scenario described above, it is reasonable to consider a more centralized approach for mobility anchor selection in order to reduce the negative effects on the control plane. If data packets are going to be tunneled in both cases, managing a single tunnel to a single mobility anchor would be better than managing several tunnels to several mobility anchors at the same time.

It is worth mentioning that the discussion above is considering applications that require IP-address continuity. On the other hand, there is no issue regarding the applications that allow an IP address change and manage mobility at the application layer since they do not need mobility anchors as mentioned before.

Some examples on this scenario are (cf. Table 1) RT gaming, audio/video conferencing, live streaming IPTV, video report, video streaming in vehicles, and camcorder download.

#### Scenario 3: running applications generating both long and short flows

In this case, short and long flows can be distinguished when selecting a mobility anchor for a flow, based on scenario 1 and scenario 2. Short flows are always anchored at the current access router; long flows are anchored based on a more centralized approach. In this way, data packets of short flows are generally routed optimally and long flows do not introduce a large number of simultaneous anchors/tunnels.

### 4.2. Mobile nodes with one or more typical locations

#### Scenario 4: running applications generating typically short flows

As the flows are short, there is no expected benefit from having a typical location. If initiated when the mobile node is not at its typical location, such flows are more likely to end quickly before the mobile node goes back to its typical location. Otherwise, they would be initiated and terminated when the mobile node is at its typical location. As a result, the current access router is always the best mobility anchor for new flows and hence the DMM default mode of mobility anchor selection fits well this scenario.

When the car is used mainly for short distance usages, Waze (cf. Table 1) could be an example on this scenario.

#### Scenario 5: running applications generating typically long flows

In this scenario, having a typical location is expected to be beneficial for the mobile node's mobility anchor selection. As mentioned before, the best mobility anchor for a flow is the closest one to the mobile node during the longer portion of this flow. Then, the best mobility anchor for a flow could be in some cases that of the typical location even if the flow is not initiated there. For example, if the mobile node initiates a long flow and then comes back (undergoing an IP-handover) quickly to its typical location, the longer portion of the flow would be after the IP-handover. Thus, it is reasonable to select the typical location's mobility anchor for such flow when initiated. This results in tunneling part of the flow's data traffic when initiated but in routing optimally most of it afterwards.

The analysis described above would be still valid if the mobile node has more than one typical location. However, the benefits may not be in some cases as great as those of the one typical location scenario, depending on the mobile node's movements. If there is no clear benefit from selecting one out of the mobility anchors, the network context (i.e. level of load on each mobility anchor) comes into play leaning towards selecting the mobility anchor that is less loaded. Another refinement is to add the time of day to the statistics collection in the mobile node's attachments history. If it is noticed that one of the typical locations is more popular than the others, this helps in selecting a mobility anchor according to the time of attachment.

Some examples on this scenario are (cf. Table 1) RT gaming, audio/video conferencing, live streaming IPTV, GoPro, video report, video streaming in vehicles, and camcorder download.

#### Scenario 6: running applications generating both long and short flows

If it is possible, the short and long flows should be distinguished as follows. While short flows are assigned the closest mobility anchor which is the current access router, long flows are assigned the typical location's mobility anchor. In this case, the mobile node uses several IP addresses simultaneously e.g. the one related to the typical location for all long flows and the current IP address for short flows. Hence, the mobile node needs a source address selection mechanism in order to distinguish between the different IP addresses when initiating a flow.

#### 4.3. Fairly stationary nodes

Scenario 7: running similar or different applications

In fact, a fairly stationary node has one typical location for almost all the time. The mobile node selects always the typical location's mobility anchor, which is the current access router most of the time.

Some examples on this scenario are (cf. Table 1) RT gaming, audio/video conferencing, live streaming IPTV, video report, and camcorder download.

## 5. Security Considerations

TBD.

## 6. IANA Considerations

This document has no actions for IANA.

## 7. Acknowledgements

The authors would like to express their gratitude to Wu-Chi Feng and Philippe Bertin for having discussions, sharing thoughts, or providing reviews on anchor selection in DMM.

## 8. References

### 8.1. Normative References

- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

### 8.2. Informative References

- [Cisco-VNI] Cisco Systems Inc., "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2009--2014", Cisco VNI , February 2010.
- [I-D.ietf-dmm-best-practices-gap-analysis] Liu, D., Zuniga, J., Seite, P., Chan, A., and C. Bernardos, "Distributed Mobility Management: Current practices and gap analysis", draft-ietf-dmm-best-practices-gap-analysis-01 (work in progress), June 2013.
- [I-D.ietf-dmm-requirements] Chan, A., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", draft-ietf-dmm-requirements-05 (work in progress), June 2013.



Authors' Addresses

Hassan Ali-Ahmad (Editor)  
Orange  
Email: hassan.aliahmad@orange.com

Danny Moses  
Intel Corporation  
Email: danny.moses@intel.com

Hassnaa Moustafa  
Intel Corporation  
Email: hassnaa.moustafa@intel.com

Pierrick Seite  
Orange  
Email: pierrick.seite@orange.com

Tiago Condexia  
University of Aveiro  
Email: tscondeixa@ua.pt



DMM  
Internet-Draft  
Intended status: Informational  
Expires: April 24, 2014

H. Chan  
Huawei Technologies  
P. Seite  
France Telecom - Orange  
K. Pentikousis  
EICT GmbH  
A. Dutta  
ATT  
October 21, 2013

Distributed Mobility Management Framework  
draft-chan-dmm-framework-03

Abstract

This document introduces a framework for mobility management protocols in terms of their key, abstract logical functions. We explain how the framework is capable of presenting a unified view, reducing the clutter that prevents a casual reader from understanding the commonalities between different approaches in mobility management. A first order application of this framework is to enable us to examine previously standardized mobility management protocols, such as MIPv6 and PMIPv6 (as well as several of their extensions), and describe their core functionality in terms of different configurations of the logical functions defined by the framework.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 24, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Conventions and Terminology . . . . .	4
3. Mobility Management Logical Functions . . . . .	4
4. Mobility Protocol Functional Decomposition . . . . .	6
4.1. Decomposing Mobile IPv6 . . . . .	6
4.2. From MIPv6 to PMIPv6 . . . . .	7
4.3. Hierarchical Mobile IPv6 . . . . .	9
4.4. Distributing Mobility Anchors . . . . .	10
4.5. Migrating Home Agents . . . . .	11
5. DMM Functional Decomposition Scenarios . . . . .	12
5.1. Flat Network Scenario . . . . .	13
5.1.1. Network-based Mobility Management . . . . .	13
5.1.2. Client-based Mobility Management . . . . .	14
5.2. DMM with Control and Data Plane Separation . . . . .	15
6. Security Considerations . . . . .	17
7. IANA Considerations . . . . .	17
8. References . . . . .	17
8.1. Normative References . . . . .	17
8.2. Informative References . . . . .	17
Appendix A. Comparing against DMM requirements . . . . .	19
A.1. First DMM requirement: distributed processing . . . . .	19
A.2. Second DMM requirement: Transparency to upper layers when needed . . . . .	20
A.3. Third DMM requirement: IPv6 deployment . . . . .	20
A.4. Fourth DMM requirement: Existing mobility protocols . . . . .	20
A.5. Fifth DMM requirement: co-existence . . . . .	20
A.6. Sixth DMM requirement: Security considerations . . . . .	20
A.7. Seventh DMM requirement: multicast . . . . .	20
Authors' Addresses . . . . .	20

## 1. Introduction

While there is ongoing research on new protocols for distributed mobility management (DMM), it has also been proposed, e.g., in [Paper-Distributed.Mobility.PMIP] and in other publications, that a DMM architecture can be designed using primarily existing mobility management protocols with some extensions. This is reflected in the requirement included in [I-D.ietf-dmm-requirements]: distributed mobility management is to first use existing protocols and their extensions before considering new protocol designs. Although this a key requirement as we move forward, it does not point to which extensions are needed let alone how to devise them.

Mobile IPv6 [RFC6275], for instance, which is a logically centralized mobility management approach addressing primarily hierarchical mobile networks, has numerous variants and extensions including, PMIPv6 [RFC5213], Hierarchical MIPv6 (HMIPv6) [RFC5380], Fast MIPv6 (FMIPv6) [RFC5568] [RFC4988], Proxy-based FMIPv6 (PFMIPv6) [RFC5949], just to name a few. These variants or extensions of MIPv6 have been developed over the years owing to the different needs that have been arising ever since the first MIP specification came into life. This document argues that we can gain much more insight into the design space of DMM protocols by abstracting the functionality of existing mobility management protocols in terms of logical functions. Different variants of existing mobility management protocols can then be expressed as different design variations of how these logical functions are put together. The result is a rich framework that can express sophisticated functionalities in a more straightforward manner. What is more, this document shows how to reconfigure these logical functions towards various distributed mobility management designs.

The rest of this document is organized as follows. After setting the stage with conventions and terminology in the following section, Section 3 introduces the framework abstractions, based on common functionality we observe in the current crop of mobility management protocols. This includes three logical functions, namely, home address allocation, routing management and location management. Such functional decomposition will enable us to clearly separate data and control plane functionality, and gives us the flexibility in an implementation to position said logical functions at their most appropriate places in the system design. Next, Section 4 shows that these logical functions can indeed perform the same functions as major existing mobility protocols. These functions therefore become the foundation for a unified framework upon which different designs of distributed mobility management may be built upon. Finally, Section 5 presents scenarios where the functional aspects of the framework are illustrated.

## 2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

All general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275] and in the Proxy Mobile IPv6 specification [RFC5213]. This includes terms such as mobile node (MN), correspondent node (CN), home agent (HA), home address (HoA), care-of-address (CoA), local mobility anchor (LMA), and mobile access gateway (MAG).

In addition, this document uses the following term:

Home network of an application session (or of an HoA) is the network that has allocated the IP address (HoA) used for the session identifier by the application running in an MN. An MN may be running multiple application sessions, and each of these sessions can have a different home network.

## 3. Mobility Management Logical Functions

Functional entity (FE) decomposition is an often-used engineering approach that enables us to look at the similarities and differences of complex systems while keeping track of their important operational aspects. Earlier work, for instance, in the European research project Ambient Networks investigated how to create an advanced and forward-looking architecture aiming primarily for mobile and wireless networks [Book-AN]. A key goal was to design mechanisms that can be deployed in a variety of settings (ad-hoc or operator-controlled) and scale from small home networks with little human supervision to sensor networks deployed over large geographical areas with limited resources, to large professionally-managed infrastructure networks. The project put forward the concept of the Ambient Control Space (ACS) which relies on only three interfaces; interested readers can find more details in [Book-AN].

Within the ACS, novel mobility management mechanisms were developed based on the concept of self-containing Functional Entities (FEs) which featured well-defined interfaces and interactions with each other. This systematic decomposition enabled the development of several mobility management mechanisms which put emphasis on different aspects. Examples of these approaches include the Generic Link Layer [Paper-GLL], Multi-radio Resource Management [Paper-MRRM], and [Paper-NODEID], which has some similarities with HIP. Later work

in this area capitalized on the established FEs within the ACS to define new mechanisms, that were not originally envisioned, such as [Paper-ANHASA].

Following this tradition, this document applies a similar approach to logically decomposing mobility management functions. This way we can establish a common framework that will enable us to reason about DMM functionality with well-defined and well-understood FEs or logical functions. As a first step, the DMM Framework presented in this document demonstrates that the existing mobility management functions of MIPv6, PMIPv6, and HMIPv6 can be abstracted into the following logical functions:

1. Session identification (SID): An MN may use an SID to enable session continuity for an application during handover. Alternatively, a separate IP address different from the routing IP address, such as that used previously in the home network where the application was initiated, may be used as the SID. Then, this function is tied to the IP prefix function at the home network. In addition, an MN with multiple ongoing applications may use multiple prefixes. This function is able to associate each prefix with the applications actively using the prefix and release the prefix when no application needs to use it anymore.
2. Location management (LM): The LM function keeps track of the internetwork location of an MN which may change its IP address as it moves. The information may associate with each SID, the IP routing address of the MN, or of a node that can forward packets destined to the MN.

In a client-server model of the system, location query and update messages may be exchanged between the client (LMc) and the server (LMs). Optionally, one (or more) proxy may exist between the LMs and the LMc, i.e., LMs-proxy-LMc. Then, to the LMs, the proxy behaves like the LMc; to the LMc, the proxy behaves like the LMs.

3. Routing Management (RM) function: In principle, it is possible to update the routing tables according to the LM information. Yet it is sometimes not practical or not scalable to update the routing tables dynamically to reflect the fast changes of locations especially when a very large number of MNs are in the Internet. The RM function is then an additional routing function beyond those provided by the routing tables, such as forwarding packets using a tunnel, rewriting a packet header to route using another IP address. It is often sufficient to have this additional function in only a limited number of special routers. Then, the RM function in these routers will need to intercept the packets to/from the MN and forward the packets, based on the

internetwork location information, either to the destination or to some other network element that knows how to forward the packets to the destination.

In addition, the Access Router (AR) logical function provides first-hop network access and includes functionality below the network layer, e.g. radio communication facilities. An AR may provide home address allocation as well as act as RM.

#### 4. Mobility Protocol Functional Decomposition

This section shows that existing mobility management protocols can be expressed as different configurations of the logical functions introduced in Section 3 above. Using these generic logical functions, we will build up the existing mobility protocols one step at a time in the following sequence: MIPv6, PMIPv6, HMIPv6, and HAHA. Functions are added and modified as needed in each step.

##### 4.1. Decomposing Mobile IPv6

Fig. 1 illustrates the Mobile IPv6 [RFC6275] functional decomposition using the logical functions introduced in Section 3. The combination of the RM, LM and HoA allocation logical functions in Network1 effectively defines the home agent or the mobility anchor. In the depicted network scenario, the mobile node designated as MN11 was originally attached to Network1 and was allocated an IP prefix for its home address (HoA11). At a later stage, MN11 moves to Network3, where it is allocated a new prefix to configure the IP address IP32. LM1 maintains the binding HoA11:IP32 so that packets from its correspondent node CN21 in Network2 destined to HoA11 can be intercepted by RM1, which will then tunnel them to IP32. MN11 must perform mobility signaling using the LU function.



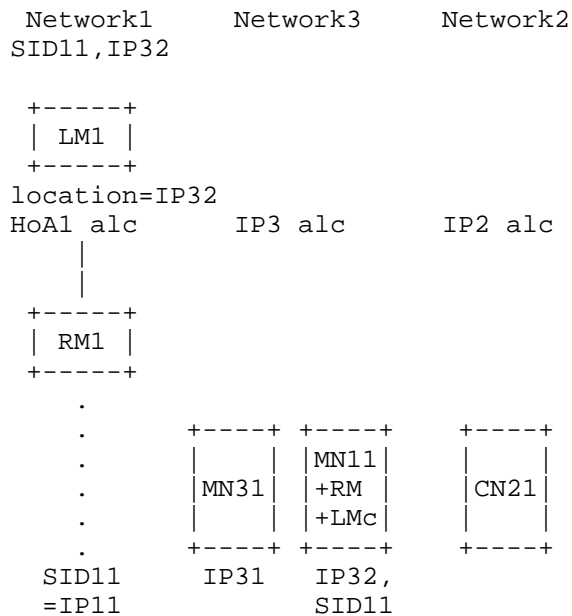


Figure 1. Functional decomposition of Mobile IPv6

#### 4.2. From MIPv6 to PMIPv6

The functional decomposition of Proxy Mobile IPv6 [RFC5213] according to the proposed framework is shown in Fig. 2. In PMIPv6, the combination of LM, RM, and HoA allocation effectively defines the Local Mobility Anchor (LMA). The combination of AR and LU together with additional signaling with MN comprises the Mobile Access Gateway (MAG). In the figure, MN11 is attached to the access router AR31 which has the IP address IP31 in Network3. LM1 maintains the binding HoA11:IP31. The access router AR31 also behaves like a home link to MN11 so that MN11 can use its original IP address HoA11.

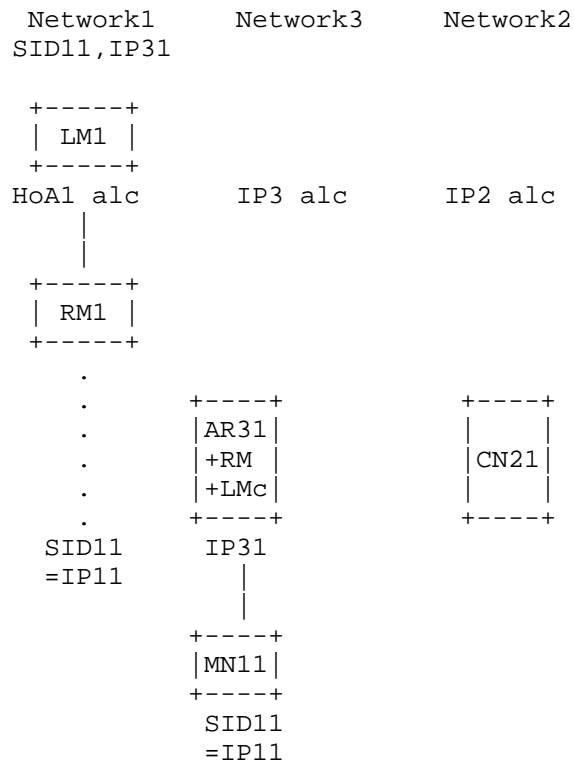


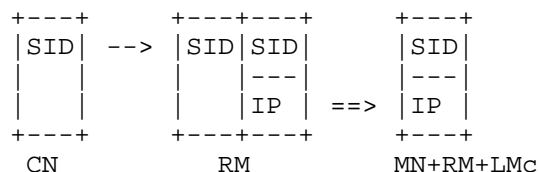
Figure 2. Functional decomposition of PMIPv6

MIPv6 and PMIPv6 both employ the same concept of separating the session identifier (HoA) from the routing address (CoA). Fig. 3 contrasts (a) MIPv6 with (b) PMIPv6 by illustrating the destination IP address in the network-layer header as a packet traverses the network from the CN to the MN. Note that MIPv6 and PMIPv6 bundle three mobility management logical functions, namely, LM1, IP1 prefix allocation and RM1 into the home agent (HA) and Local Mobility Anchor (LMA), respectively.

Fig. 3 shows that, as far as data-plane traffic is concerned, routing from CN to MN+LU in MIPv6 is similar to the route from CN to AR+LU in PMIPv6. The difference is in that in the former case, the MN with the LU function is substituted by the combination of the AR with the LU function and the MN. While additional signaling is needed to enable the combination of AR+LU and MN to behave like MN+LU in MIPv6, such signaling can be confined between the AR+LU and the MN only. It can therefore be seen under this unified formulation, that a host-based mobility management protocol can be translated using this substitution into a network-based mobility management protocol and

vice versa.

(a) MIPv6:



(b) PMIPv6:

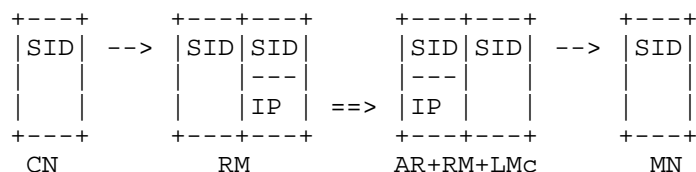


Figure 3. Network layer in the protocol stack of packets sent from the CN and tunneled (a) to the MN+RM+LMc in MIPv6; and (b) to the AR+RM+LMc in PMIPv6 showing the destination IP address as the packet traverses from the CN to the MN.

#### 4.3. Hierarchical Mobile IPv6

The functional decomposition of Hierarchical Mobile IPv6 [RFC5380] is shown in Fig. 4. Besides the logical functions LM1, RM1, and HoA1 prefix allocation in Network1, as we have seen above for MIPv6 and PMIPv6, there is an RM function (RM3) in the visited network (Network3). RM3 acts also as a proxy between LM1 and MN11 in the hierarchical LM function LM1--RM3--MN11. That is, LM1 maintains the LM binding HoA11:RM3 while RM3 tracks the LM binding HoA11:IP32. The combined function of RM and the LM proxy function is the Mobility Anchor Point (MAP).

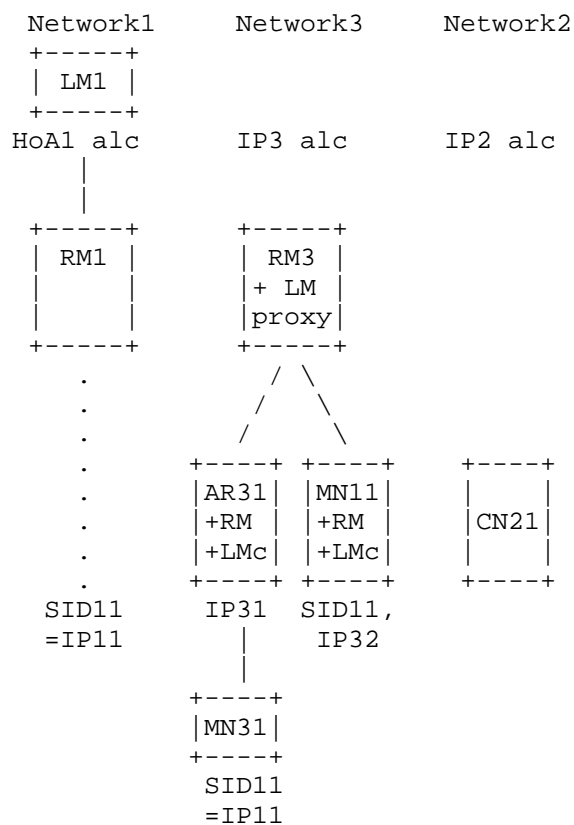


Figure 4. Functional decomposition of Hierarchical Mobile IPv6

Note that as depicted in Fig. 4, if MN11 takes the place of MN31 which is attached to AR31, the resulting mobility management becomes network-based.

#### 4.4. Distributing Mobility Anchors

As we have seen so far, the framework is sufficiently expressive to enable us to decompose the major MIPv6 variants. It is possible to replicate the mobility anchoring function for any of MIPv6, PMIPv6, or HMIPv6, in multiple networks as shown in Fig. 5 which illustrates such an example with three networks.

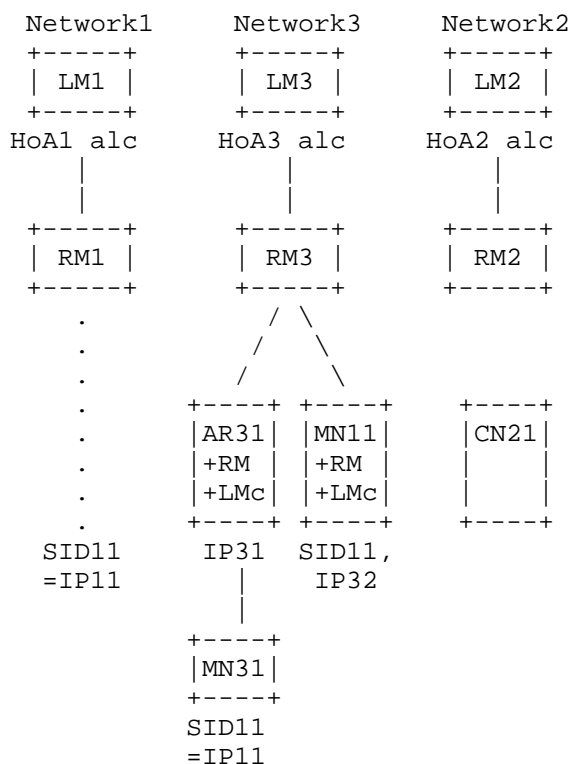


Figure 5. Distributing mobility anchors using the DMM Framework logical functions

#### 4.5. Migrating Home Agents

When all logical functions of the Framework are bundled into a single entity e.g., a home agent in MIPv6 or a local mobility anchor in PMIPv6, in a single network, the result is triangular routing when the MN and the CN are in networks close to each other but are far from the anchor point. A method to solve the triangle routing problem is to duplicate the anchor points in many networks in different geographic locations as advocated in [Paper-Migrating.Home.Agents]. A functional decomposition of Migrating Home Agents is shown in Fig. 6: the RM function is available in each of the three networks Network1, Network2, and Network3. The LM function in each network (LM0) contains the LM information for all three networks. Each RM in each network advertises the HoA IP prefixes of all these networks using anycast. Traffic from CN21 in Network2 destined to HoA11 will therefore be intercepted by the RM nearest to the CN, i.e. RM2 in the example of Fig. 6. Using the LM information in LM0, RM2 will use the binding

HoA1:IP32 to tunnel the packets to MN11.

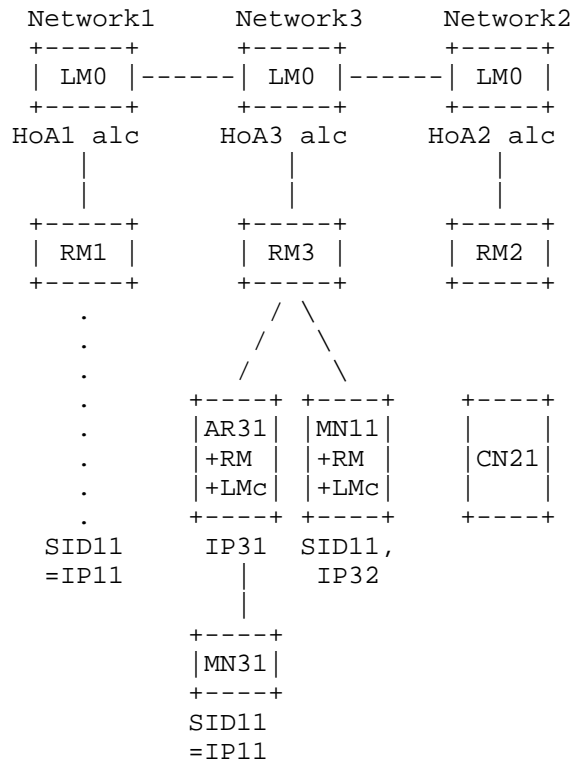


Figure 6. Functional decomposition of Migrating Home Agents

Similarly, traffic originating from MN11 will be served by its nearest RM (RM3). Triangular routing is therefore avoided. Yet the synchronization of all home agents becomes a challenge as discussed in [Paper-SMGI]. In addition, the amount of signaling traffic necessary for synchronizing the home agents may become excessive when both the number of mobile nodes and the number of home agents increase.

As before, if MN11 in Fig. 6 takes the place of MN31 which is attached to AR31, the resulting mobility management becomes network-based.

## 5. DMM Functional Decomposition Scenarios

This section covers the functional description of DMM. Basically,

the scenarios present a way to distribute the logical mobility functions.

#### 5.1. Flat Network Scenario

In a flat network, the logical functions may all be located at the AR as shown in Figs. 7 and 8, respectively. For example, [I-D.seite-dmm-dma] and [I-D.bernardos-dmm-distributed-anchoring] are PMIPv6-based implementations of this scenario. These two figures depict the network- and client-based distributed mobility management scenarios, respectively. AR is expected to support the HoA allocation function. Then, depending on the mobility situation of the MN, the AR can run different functions:

1. AR can act as a standard IP router;
2. AR can provide the RM function (i.e. act as mobility anchor);
3. AR can provide the LU function;
4. AR can provide both RM and LU functions.

##### 5.1.1. Network-based Mobility Management

The functional decomposition of network-based mobility management is depicted in Fig. 7. In case (1), MN1 attaches to AR1. AR advertises the prefix HoA1 to MN1 and then acts as a legacy IP router. MN1 initiates a communication with CN11.

In case (2), MN1 performs a handover from AR1 to AR3 while maintaining ongoing IP communication with CN11. AR1 becomes the mobility anchor for the MN1-CN11 IP communication: AR1 runs RM and LM functions on behalf of MN1. AR3 performs LU up to the LM in AR1: AR3 indicates to AR1 the new location of the MN1. AR3 allocates a new IP prefix (HoA3) for new IP communications. That is, HoA3 is used for all new IP communications, e.g., if MN1 initiates IP communication with CN21. AR3 shall act as a legacy IP router for MN1-CN21 communication.

In case (3), MN1 performs a handover from AR1 to AR2 with ongoing IP communication with CN11 and CN21. AR1 is the mobility anchor for the MN1-CN11 IP communication. AR3 becomes the mobility anchor for the MN1-CN21 IP communication. Both AR1 and AR3 run RM and LM functions for MN1, respectively, anchoring HoA1 and HoA3. AR2 performs location updates up to the LMs in AR1 and AR3 for respectively relocate HoA1 and HoA3.

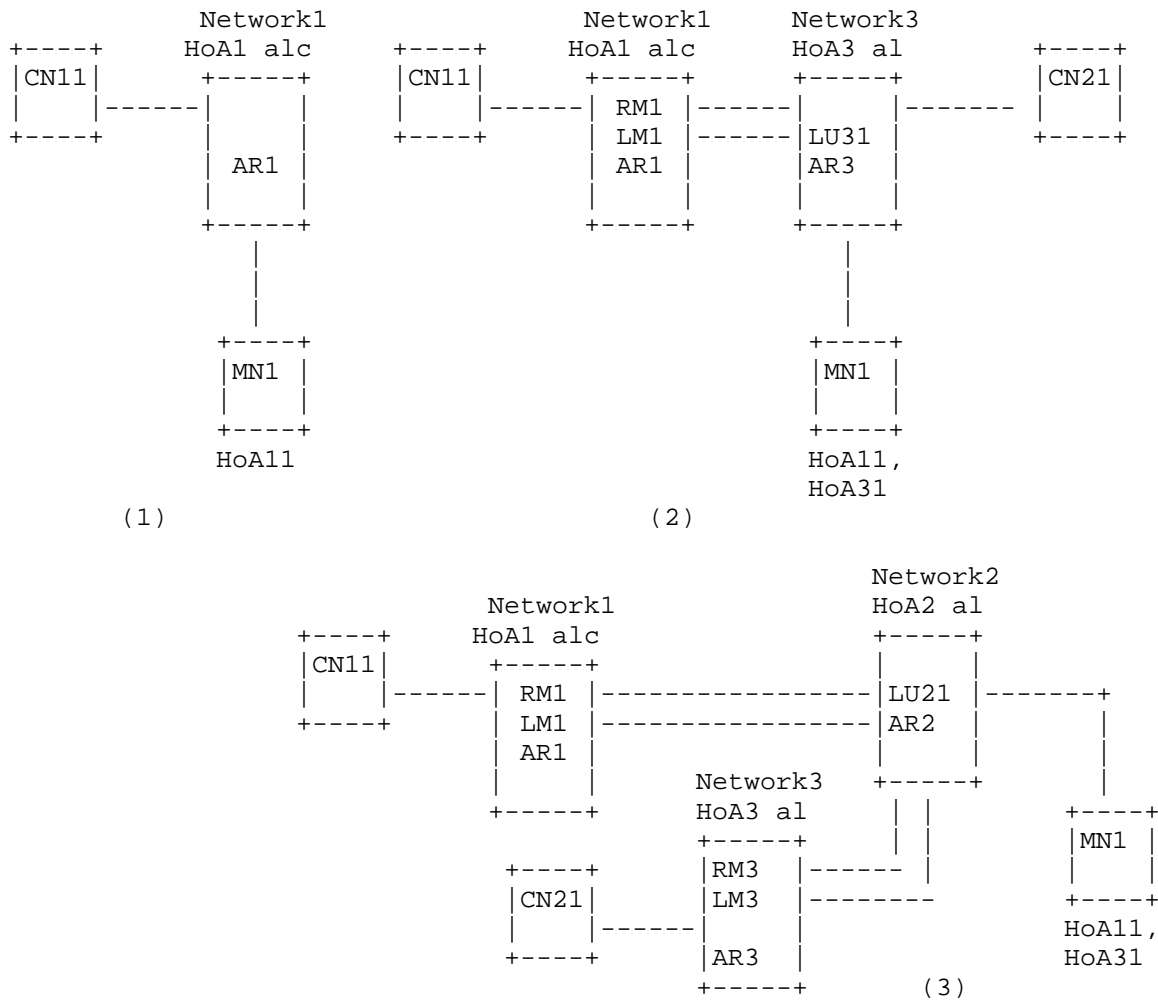


Figure 7. Network-based DMM architecture for a flat network

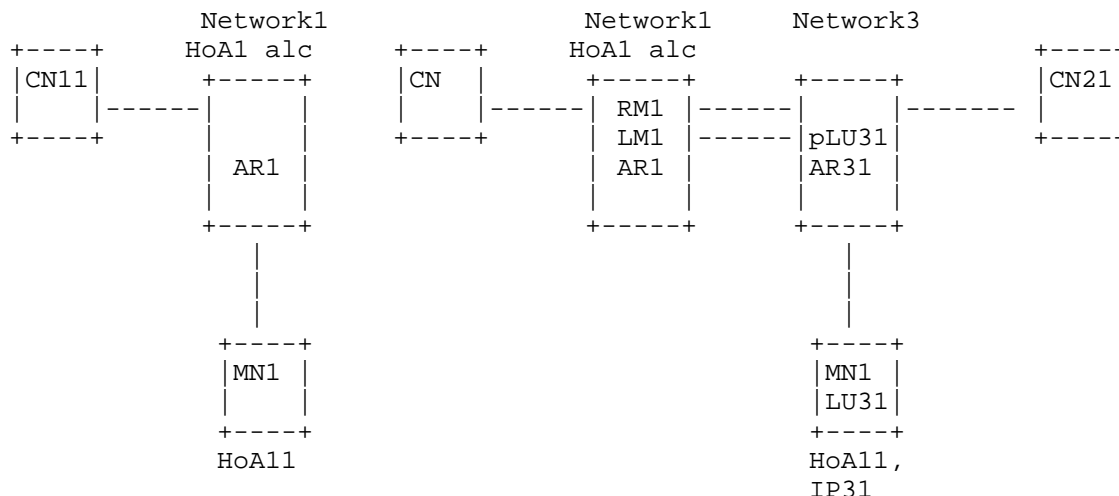
#### 5.1.2. Client-based Mobility Management

The functional decomposition of client-based mobility management is depicted in Fig. 8. In case (1), MN1 attaches to AR1. AR advertises the prefix HoA1 to MN1 and then acts as a legacy IP router. MN1 initiates a communication with CN11.

In case (2), MN1 performs a handover from AR1 to AR3 while maintaining ongoing IP communication with CN11. AR1 becomes the mobility anchor for the MN1-CN11 IP communication: AR1 runs RM and LM functions for MN1. The MN performs LU directly up to the LM in AR1



or via AR3; in this case AR3 acts as a proxy locator (pLU) (e.g. as a FA in MIPv4). AR3 allocates a new IP prefix (HoA3) for new IP communications. HoA3 is supposed to be used for new IP communications, e.g., if MN1 initiates IP communication with CN21. AR3 shall act as a legacy IP router for MN1-CN21 communication.



(1)

(2)

Figure 8. Client-based DMM architecture for a flat network

## 5.2. DMM with Control and Data Plane Separation

This section considers a scenario which involves multiple RMs and a distributed LM database. The different use case scenarios of distributed mobility management are described in [I-D.yokota-dmm-scenario] as well as in [Paper-Distributed.Mobility.Review]. The functional decomposition described in this document can be used to understand better the data and control plane separation.

Fig. 9 shows an example DMM topology with the same three networks we have been using in Fig. 5. As in Fig. 5, each network in Fig. 9 has its own IP prefix allocation function. In the data plane, the routing management function is distributed to multiple locations at the RMs so that routing can be optimized. In the control plane, the RMs may exchange information with each other.

In addition to these features, the LM function in Fig. 9 is a distributed database, possibly implemented with multiple virtual or physical servers, handling the mapping of HoA to CoA. To perform

routing management, the RMs need the location information which is maintained at LM1, LM2, and LM3. The RMs are, therefore, the clients of the LM servers and may also send location updates to the LM as the MNs perform the handover. The location information may either be pulled from the LM servers by the RM, or pushed to the RM by the LM servers. In addition, the RM may also cache a limited amount of location information.

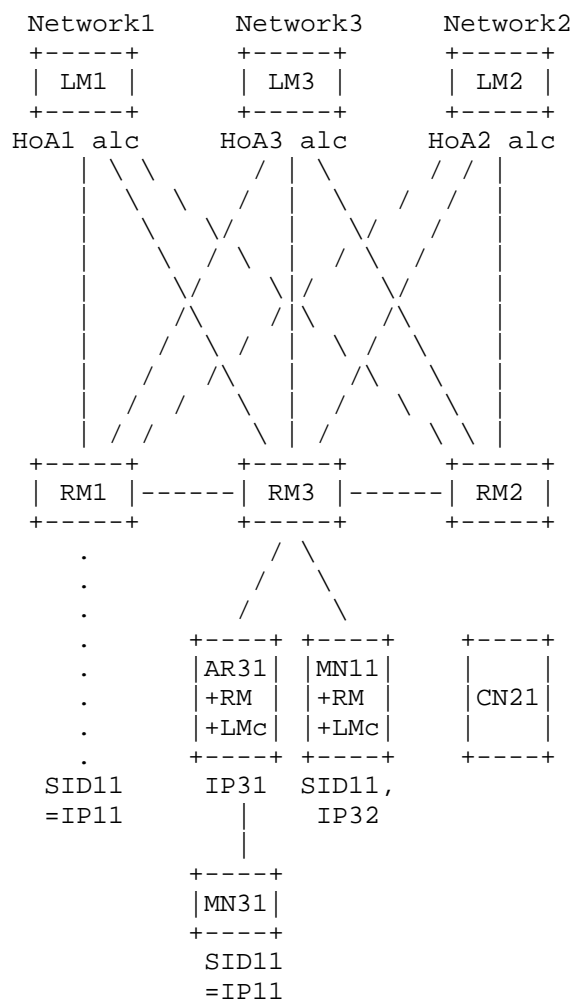


Figure 9. DMM with Control and Data Plane Separation

Fig. 9 illustrates three RMs (RM1, RM2, and RM3) in three networks. In this scenario we take that MN11 has moved from Network1 supported

by RM1 and LM1 to Network3 supported by RM3 and LM3. MN11 may use the home address (HoA11) allocated to it when it was directly connected to the former network for those application sessions that were started when the mobile node was attached there and do require session continuity after the handover to the latter network. When MN11 is connected to Network1, no location management is needed; LM1 will not keep an entry for HoA11. After MN11 handovers to Network3, the LM1 server maintains a mapping of HoA11 to RM3. That is, LM1 points to Network3 and it is this network that will keep track of how to reach MN11. Such a hierarchical mapping can prevent frequent signaling updates to LM1, as MN11 performs intra-network handover(s) within the Network3 domain. In other words, the concept of hierarchical mobile IP [RFC5380] is applied here for location management only but not for data plane routing.

## 6. Security Considerations

TBD

## 7. IANA Considerations

This document presents no IANA considerations.

## 8. References

### 8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

### 8.2. Informative References

[Book-AN] Niebert, N., Schieder, A., Zander, J., and R. Hancock (Eds.), "Ambient networks: co-operative mobile networking for the wireless world.", Wiley, 2007.

[I-D.bernardos-dmm-distributed-anchoring]  
Bernardos, CJ. and JC. Zuniga, "PMIPv6-based distributed anchoring", draft-bernardos-dmm-distributed-anchoring-01 (work in progress), September 2012.

[I-D.ietf-dmm-requirements]  
Chan (Ed.) et al., H., "Requirements for Distributed Mobility Management", draft-ietf-dmm-requirements-06 (work in progress), December 2012.

- [I-D.seite-dmm-dma]  
Seite, P., Bertin, P., and JH. Lee, "Distributed Mobility Anchoring", draft-seite-dmm-dma-06 (work in progress), January 2013.
- [I-D.yokota-dmm-scenario]  
Yokota, H., Seite, P., Demaria, E., and Z. Cao, "Use case scenarios for Distributed Mobility Management", draft-yokota-dmm-scenario-00 (work in progress), October 2010.
- [Paper-ANHASA]  
Pentikousis, K., Agüero, R., Gebert, J., Galache, J., Blume, O., and P. Paakkonen, "The Ambient Networks heterogeneous access selection architecture", Mobility, Multiaccess, and Network Management (M2NM) 2007. First Ambient Networks Workshop on. Sydney, Australia, October 2007, pp. 49-54, October 2007.
- [Paper-Distributed.Mobility.PMIP]  
Chan, H., "Proxy Mobile IP with Distributed Mobility Anchors", Proceedings of GlobeCom Workshop on Seamless Wireless Mobility, December 2010.
- [Paper-Distributed.Mobility.Review]  
Chan, H., Yokota, H., Xie, J., Seite, P., and D. Liu, "Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues", February 2011.
- [Paper-GLL]  
Koudouridis, G., Agüero, R., Alexandri, E., Choque, J., Dimou, K., Karimi, H., Lederer, H., Sachs, J., and R. Sigle, "Generic link layer functionality for multi-radio access networks", Proc. IST Mobile and Wireless Communication Summit 2005., 2005.
- [Paper-MRRM]  
Berggren, F., Bria, A., Badia, L., Karla, I., Litjens, R., Magnusson, P., Meago, F., Tang, H., and R. Veronesi, "Multi-radio resource management for ambient networks", Personal, Indoor and Mobile Radio Communications (PIMRC) 2005. IEEE 16th International Symposium on. Vol. 2, pp. 942-946, 2005.
- [Paper-Migrating.Home.Agents]  
Wakikawa, R., Valadon, G., and J. Murai, "Migrating Home Agents Towards Internet-scale Mobility Deployments", Proceedings of the ACM 2nd CoNEXT Conference on Future

Networking Technologies, December 2006.

[Paper-NODEID]

Ahlgren, B., Eggert, L., Ohlman, B., and A. Schieder, "Ambient networks: Bridging heterogeneous network domains", Personal, Indoor and Mobile Radio Communications (PIMRC) 2005. IEEE 16th International Symposium on. Vol. 2, pp. 937-941, 2005.

[Paper-SMGI]

Zhang, L., Wakikawa, R., and Z. Zhu, "Support Mobility in the Global Internet", Proceedings of ACM Workshop on MICNET, MobiCom 2009, Beijing, China, September 2009.

[RFC4988] Koodli, R. and C. Perkins, "Mobile IPv4 Fast Handovers", RFC 4988, October 2007.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

[RFC5568] Koodli, R., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.

[RFC5949] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 2010.

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

## Appendix A. Comparing against DMM requirements

This section examines how the framework meets the DMM requirements.

### A.1. First DMM requirement: distributed processing

The framework has defined a set of mm functions which can be implemented in a distributed fashion. As further evidence, the document explains how the mm functions can be used to implement in a distributed manner the major mm protocols (MIPv6, PMIPv6, HMIP, DMA, MHA).

A.2. Second DMM requirement: Transparency to upper layers when needed

In the framework, transparency depends on how the RM functions is implemented. This draft has already shown that using the framework one can express, for example, PMIP and DMA, which are transparent to the upper layers.

A.3. Third DMM requirement: IPv6 deployment

The framework is not tied to a particular IP version, and therefore supports IPv6 deployment.

A.4. Fourth DMM requirement: Existing mobility protocols

This draft has already described how to express the functionality of several mm protocols (MIPv6, PMIPv6, HMIP, DMA, MHA). More cases can be added as feedback is received.

A.5. Fifth DMM requirement: co-existence

The framework enables the expression of existing protocols in functions that can be extended to provide distributed mobility support, and can be made backwards compatible with existing implementations.

A.6. Sixth DMM requirement: Security considerations

Security risks are associated with the particular DMM solution. The framework is flexible and does not restrict DMM solutions in a way that the DMM solution can increase security risks.

A.7. Seventh DMM requirement: multicast

It appears possible to extend the framework by decomposing multimob solutions with the framework.

Authors' Addresses

H Anthony Chan  
Huawei Technologies  
5340 Legacy Dr. Building 3  
Plano, TX 75024  
USA

Email: h.a.chan@ieee.org

Pierrick Seite  
France Telecom - Orange  
4, rue du Clos Courtel, BP 91226  
Cesson-Sevigne 35512  
France

Email: [pierrick.seite@orange-ftgroup.com](mailto:pierrick.seite@orange-ftgroup.com)

Kostas Pentikousis  
EICT GmbH

Email: [k.pentikousis@eict.de](mailto:k.pentikousis@eict.de)

Ashutosh Dutta  
ATT  
200 Laurel Ave S  
Middletown, NJ 07748  
USA

Email: [ashutosh.dutta@ieee.org](mailto:ashutosh.dutta@ieee.org)





DMM  
Internet-Draft  
Intended status: Informational  
Expires: May 8, 2015

D. Liu, Ed.  
China Mobile  
JC. Zuniga, Ed.  
InterDigital  
P. Seite  
Orange  
H. Chan  
Huawei Technologies  
CJ. Bernardos  
UC3M  
November 4, 2014

Distributed Mobility Management: Current practices and gap analysis  
draft-ietf-dmm-best-practices-gap-analysis-09

Abstract

This document analyzes deployment practices of existing IP mobility protocols in a distributed mobility management environment. It then identifies existing limitations when compared to the requirements defined for a distributed mobility management solution.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 8, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Terminology . . . . .	3
3. Functions of existing mobility protocols . . . . .	3
4. DMM practices . . . . .	5
4.1. Assumptions . . . . .	5
4.2. IP flat wireless network . . . . .	6
4.2.1. Host-based IP DMM practices . . . . .	7
4.2.2. Network-based IP DMM practices . . . . .	11
4.3. Flattening 3GPP mobile network approaches . . . . .	13
5. Gap analysis . . . . .	16
5.1. Distributed mobility management - REQ1 . . . . .	16
5.2. Bypassable network-layer mobility support for each application session - REQ2 . . . . .	19
5.3. IPv6 deployment - REQ3 . . . . .	20
5.4. Considering existing mobility protocols - REQ4 . . . . .	20
5.5. Coexistence with deployed networks/hosts and operability across different networks - REQ5 . . . . .	21
5.6. Operation and management considerations - REQ6 . . . . .	21
5.7. Security considerations - REQ7 . . . . .	22
5.8. Multicast - REQ8 . . . . .	22
5.9. Summary . . . . .	23
6. Security Considerations . . . . .	25
7. Contributors . . . . .	25
8. References . . . . .	26
8.1. Normative References . . . . .	26
8.2. Informative References . . . . .	26
Authors' Addresses . . . . .	30

## 1. Introduction

Existing network-layer mobility management protocols have primarily employed a mobility anchor to ensure connectivity of a mobile node by forwarding packets destined to, or sent from, the mobile node after the node has moved to a different network. The mobility anchor has been centrally deployed in the sense that the traffic of millions of mobile nodes in an operator network is typically managed by the same anchor. This centralized deployment of mobility anchors to manage IP sessions poses several problems. In order to address these problems, a distributed mobility management (DMM) architecture has been

proposed. This document investigates whether it is feasible to deploy current IP mobility protocols in a DMM scenario in a way that can fulfill the requirements as defined in [RFC7333]. It discusses current deployment practices of existing mobility protocols and identifies the limitations (gaps) in these practices from the standpoint of satisfying DMM requirements. The analysis is primarily towards IPv6 deployment, but can be seen to also apply to IPv4 whenever there are IPv4 counterparts equivalent to the IPv6 mobility protocols.

The rest of this document is organized as follows. Section 3 analyzes existing IP mobility protocols by examining their functions and how these functions can be configured and used to work in a DMM environment. Section 4 presents the current practices of IP wireless networks and 3GPP architectures. Both network- and host-based mobility protocols are considered. Section 5 presents the gap analysis with respect to the current practices.

## 2. Terminology

All general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275], in the Proxy Mobile IPv6 specification [RFC5213], and in the Distributed Mobility Management Requirements [RFC7333]. These terms include mobile node (MN), correspondent node (CN), home agent (HA), Local Mobility Anchor (LMA), Mobile Access Gateway (MAG), centrally deployed mobility anchors, distributed mobility management, hierarchical mobile network, flatter mobile network, and flattening mobile network.

In addition, this document also introduces some definitions of IP mobility functions in Section 3.

In this document there are also references to a "distributed mobility management environment." By this term, we refer to a scenario in which the IP mobility, access network and routing solutions allow for setting up IP networks so that traffic is distributed in an optimal way, without relying on centrally deployed mobility anchors to manage IP mobility sessions.

## 3. Functions of existing mobility protocols

The host-based Mobile IPv6 (MIPv6) [RFC6275] and its network-based extension, Proxy Mobile IPv6 (PMIPv6) [RFC5213], as well as Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] are logically centralized mobility management approaches addressing primarily hierarchical mobile networks. Although these approaches are centralized, they have important mobility management functions resulting from years of

extensive work to develop and to extend these functions. It is therefore useful to take these existing functions and examine them in a DMM scenario in order to understand how to deploy the existing mobility protocols to provide distributed mobility management.

The main mobility management functions of MIPv6, PMIPv6, and HMIPv6 are the following:

1. Anchoring Function (AF): allocation to a mobile node of an IP address, i.e., Home Address (HoA), or prefix, i.e., Home Network Prefix (HNP) topologically anchored by the advertising node. That is, the anchor node is able to advertise a connected route into the routing infrastructure for the allocated IP prefixes. This function is a control plane function.
2. Internetwork Location Information (LI) function: managing and keeping track of the internetwork location of an MN. The location information may be a binding of the IP advertised address/prefix, e.g., HoA or HNP, to the IP routing address of the MN or of a node that can forward packets destined to the MN. It is a control plane function.

In a client-server protocol model, location query and update messages may be exchanged between a location information client (LIc) and a location information server (LIs).

3. Forwarding Management (FM) function: packet interception and forwarding to/from the IP address/prefix assigned to the MN, based on the internetwork location information, either to the destination or to some other network element that knows how to forward the packets to their destination.

FM may optionally be split into the control plane (FM-CP) and data plane (FM-DP).

In Mobile IPv6, the home agent (HA) typically provides the anchoring function (AF); the location information server (LIs) is at the HA whereas the location information client (LIc) is at the MN; the Forwarding Management (FM) function is distributed between the ends of the tunnel at the HA and the MN.

In Proxy Mobile IPv6, the Local Mobility Anchor (LMA) provides the anchoring function (AF); the location information server (LIs) is at the LMA whereas the location information client (LIc) is at the mobile access gateway (MAG); the Forwarding Management (FM) function is distributed between the ends of the tunnel at the HA and the MAG.

In Hierarchical Mobile IPv6 (HMIPv6) [RFC5380], the Mobility Anchor Point (MAP) serves as a location information aggregator between the LIs at the HA and the LIc at the MN. The MAP also provides the FM function to enable tunneling between HA and itself as well as tunneling between MN and itself.

#### 4. DMM practices

This section documents deployment practices of existing mobility protocols to satisfy distributed mobility management requirements. This description considers both IP wireless, e.g., evolved Wi-Fi hotspots, and 3GPP flattening mobile network.

While describing the current DMM practices, the section provides references to the generic mobility management functions described in Section 3 as well as some initial hints on the identified gaps with respect to the DMM requirements documented in [RFC7333].

##### 4.1. Assumptions

There are many different approaches that can be considered to implement and deploy a distributed anchoring and mobility solution. The focus of the gap analysis is on certain current mobile network architectures and standardized IP mobility solutions, considering any kind of deployment options which do not violate the original protocol specifications. In order to limit the scope of our analysis of DMM practices, we consider the following list of technical assumptions:

1. Both host- and network-based solutions are considered.
2. Solutions should allow selecting and using the most appropriate IP anchor among a set of available candidates.
3. Mobility management should be realized by the preservation of the IP address across the different points of attachment (i.e., provision of IP address continuity). This is in contrast to certain transport-layer based approaches such as Stream Control Transmission Protocol (SCTP) [RFC4960] or application-layer mobility.

Applications which can cope with changes in the MN's IP address do not depend on IP mobility management protocols such as DMM. Typically, a connection manager together with the operating system will configure the source address selection mechanism of the IP stack. This might involve identifying application capabilities and triggering the mobility support accordingly. Further considerations on application management and source address selection are out of the scope of this document, but the reader might consult [RFC6724].

## 4.2. IP flat wireless network

This section focuses on common IP wireless network architectures and how they can be flattened from an IP mobility and anchoring point of view using common and standardized protocols. We take Wi-Fi as an useful wireless technology, since it is widely known and deployed nowadays. Some representative examples of Wi-Fi deployment architectures are depicted in Figure 1.

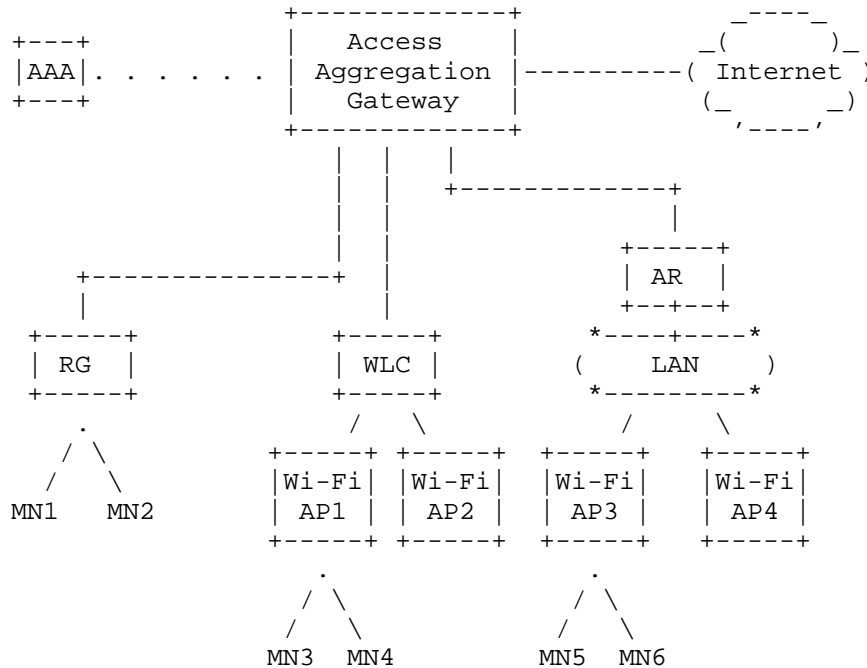


Figure 1: IP Wi-Fi network architectures

In Figure 1, three typical deployment options are shown [I-D.gundavelli-v6ops-community-wifi-svcs]. On the left hand side of the figure, mobile nodes MN1 and MN2 directly connect to a Residential Gateway (RG) at the customer premises. The RG hosts the 802.11 Access Point (AP) function to enable wireless layer-2 access connectivity and also provides layer-3 routing functions. In the middle of the figure, mobile nodes MN3 and MN4 connect to Wi-Fi Access Points (APs) AP1 and AP2 that are managed by a Wireless LAN Controller (WLC), which performs radio resource management on the APs, domain-wide mobility policy enforcement and centralized forwarding function for the user traffic. The WLC could also implement layer-3 routing functions, or attach to an access router (AR). Last, on the right-hand side of the figure, access points AP3

and AP4 are directly connected to an access router. This can also be used as a generic connectivity model.

IP mobility protocols can be used to provide heterogeneous network mobility support to users, e.g., handover from Wi-Fi to cellular access. Two kinds of protocols can be used: Proxy Mobile IPv6 [RFC5213] or Mobile IPv6 [RFC5555], with the role of mobility anchor, e.g., Local Mobility Anchor or home agent, typically being played by the edge router of the mobile network [SDO-3GPP.23.402].

Although this section has made use of the example of Wi-Fi networks, there are other flattening mobile network architectures specified, such as WiMAX [IEEE.802-16.2009], which integrates both host- and network-based IP mobility functions.

Existing IP mobility protocols can also be deployed in a flatter manner, so that the anchoring and access aggregation functions are distributed. We next describe several practices for the deployment of existing mobility protocols in a distributed mobility management environment. The analysis in this section is limited to protocol solutions based on existing IP mobility protocols, either host- or network-based, such as Mobile IPv6 [RFC6275], [RFC5555], Proxy Mobile IPv6 (PMIPv6) [RFC5213], [RFC5844] and Network Mobility Basic Support protocol (NEMO) [RFC3963]. Extensions to these base protocol solutions are also considered. The analysis is divided into two parts: host- and network-based practices.

#### 4.2.1. Host-based IP DMM practices

Mobile IPv6 (MIPv6) [RFC6275] and its extension to support mobile networks, the NEMO Basic Support protocol (hereafter, simply referred to as NEMO) [RFC3963] are well-known host-based IP mobility protocols. They depend on the function of the Home Agent (HA), a centralized anchor, to provide mobile nodes (hosts and routers) with mobility support. In these approaches, the Home Agent typically provides the Anchoring Function (AF), Forwarding Management (FM), and Internetwork Location Information server (LIS) functions. The mobile node possesses the Location Information client (LIC) function and the FM function to enable tunneling between HA and itself. We next describe some practices that show how MIPv6/NEMO and several other protocol extensions can be deployed in a distributed mobility management environment.

One approach to distribute the anchors can be to deploy several HAs (as shown in Figure 2), and assign the topologically closest anchor to each MN [RFC4640], [RFC5026], [RFC6611]. In the example shown in Figure 2, the mobile node MN1 is assigned to the home agent HA1 and uses a home address anchored by HA1 to communicate with the

correspondent node CN1. Similarly, the mobile node MN2 is assigned to the home agent HA2 and uses a home address anchored by HA2 to communicate with the correspondent node CN2. Note that MIPv6/NEMO specifications do not prevent the simultaneous use of multiple home agents by a single mobile node. In this deployment model, the mobile node can use several anchors at the same time, each of them anchoring IP flows initiated at a different point of attachment. However, there is currently no mechanism specified in IETF standard to enable an efficient dynamic discovery of available anchors and the selection of the most suitable one.

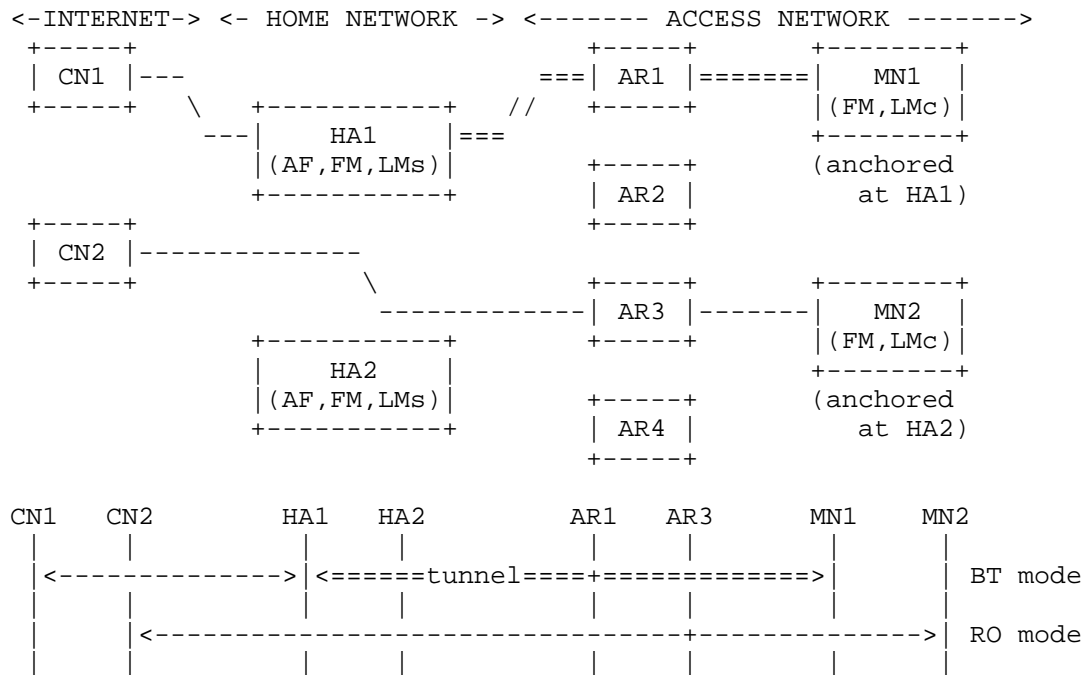


Figure 2: Distributed operation of Mobile IPv6 (BT and RO) / NEMO

One goal of the deployment of mobility protocols in a distributed mobility management environment is to avoid the suboptimal routing caused by centralized anchoring. Here, the Route Optimization (RO) support provided by Mobile IPv6 can be used to achieve a flatter IP data forwarding. By default, Mobile IPv6 and NEMO use the so-called Bidirectional Tunneling (BT) mode, in which data traffic is always encapsulated between the MN and its HA before being directed to any other destination. The RO mode allows the MN to update its current location on the CNs, and then use the direct path between them. Using the example shown in Figure 2, MN1 is using BT mode with CN1,



while MN2 is in RO mode with CN2. However, the RO mode has several drawbacks:

- o The RO mode is only supported by Mobile IPv6. There is no route optimization support standardized for the NEMO protocol because of the security problems posed by extending return routability tests for prefixes, although many different solutions have been proposed [RFC4889].
- o The RO mode requires signaling that adds some protocol overhead.
- o The signaling required to enable RO involves the home agent and is repeated periodically for security reasons [RFC4225]. Therefore the HA remains a single point of failure.
- o The RO mode requires support from the CN.

Notwithstanding these considerations, the RO mode does offer the possibility of substantially reducing traffic through the Home Agent, in cases when it can be supported by the relevant correspondent nodes. Note that a mobile node can also use its care-of-address (CoA) directly [RFC5014] when communicating with CNs on the same link or anywhere in the Internet, although no session continuity support would be provided by the IP stack in this case.

Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] (as shown in Figure 3), is another host-based IP mobility extension which can be considered as a complement to provide a less centralized mobility deployment. It allows the reduction of the amount of mobility signaling as well as improving the overall handover performance of Mobile IPv6 by introducing a new hierarchy level to handle local mobility. The Mobility Anchor Point (MAP) entity is introduced as a local mobility handling node deployed closer to the mobile node. It provides LI intermediary function between the LI server (LIs) at the HA and the LI client (LIc) at the MN. It also performs the FM function to tunnel with the HA and also with the MN.

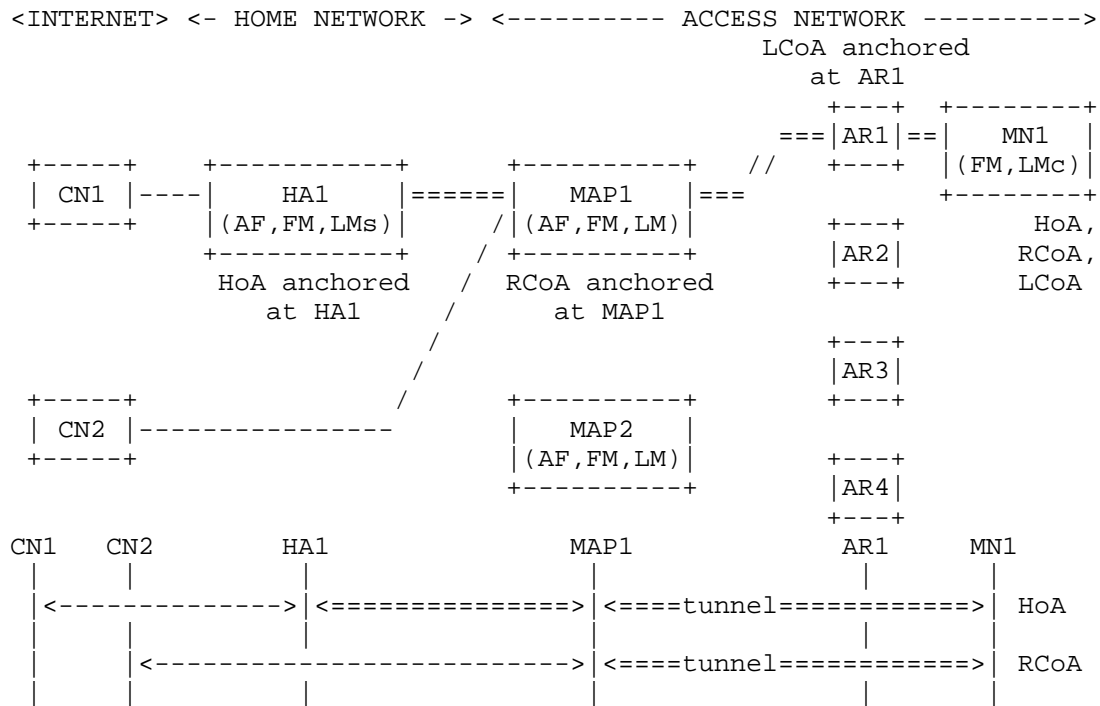


Figure 3: Hierarchical Mobile IPv6

When HMIPv6 is used, the MN has two different temporary addresses: the Regional Care-of Address (RCoA) and the Local Care-of Address (LCoA). The RCoA is anchored at one MAP, which plays the role of local home agent, while the LCoA is anchored at the access router level. The mobile node uses the RCoA as the CoA signaled to its home agent. Therefore, while roaming within a local domain handled by the same MAP, the mobile node does not need to update its home agent, i.e., the mobile node does not change its RCoA.

The use of HMIPv6 enables a form of route optimization, since a mobile node may decide to directly use the RCoA as source address for a communication with a given correspondent node, particularly if the MN does not expect to move outside the local domain during the lifetime of the communication. This can be seen as a potential DMM mode of operation, though it fails to provide session continuity if and when the MN moves outside the local domain. In the example shown in Figure 3, MN1 is using its global HoA to communicate with CN1, while it is using its RCoA to communicate with CN2.

Furthermore, a local domain might have several MAPs deployed, enabling therefore a different kind of HMIPv6 deployments which are

flattening and distributed. The HMIPv6 specification supports a flexible selection of the MAP, including those based on the distance between the MN and the MAP, or taking into consideration the expected mobility pattern of the MN.

Another extension that can be used to help with distributing mobility management functions is the Home Agent switch specification [RFC5142], which defines a new mobility header for signaling a mobile node that it should acquire a new home agent. [RFC5142] does not specify the case of changing the mobile node's home address, as that might imply loss of connectivity for ongoing persistent connections. Nevertheless, that specification could be used to force the change of home agent in those situations where there are no active persistent data sessions that cannot cope with a change of home address.

There are other host-based approaches standardized that can be used to provide mobility support. For example MOBIKE [RFC4555] allows a mobile node encrypting traffic through IKEv2 [RFC5996] to change its point of attachment while maintaining a Virtual Private Network (VPN) session. The MOBIKE protocol allows updating the VPN Security Associations (SAs) in cases where the base connection initially used is lost and needs to be re-established. The use of the MOBIKE protocol avoids having to perform an IKEv2 re-negotiation. Similar considerations to those made for Mobile IPv6 can be applied to MOBIKE; though MOBIKE is best suited for situations where the address of at least one endpoint is relatively stable and can be discovered using existing mechanisms such as DNS.

Extensions have been defined to the mobility protocol to optimize the handover performance. Mobile IPv6 Fast Handovers (FMIPv6) [RFC5568] is the extension to optimize handover latency. It defines new access router discovery mechanism before handover to reduce the new network discovery latency. It also defines a tunnel between the previous access router and the new access router to reduce the packet loss during handover. The Candidate Access Router Discovery (CARD) [RFC4066] and Context Transfer Protocol (CTXP) [RFC4067] protocols were standardized to improve the handover performance. The DMM deployment practice discussed in this section can also use those extensions to improve the handover performance.

#### 4.2.2. Network-based IP DMM practices

Proxy Mobile IPv6 (PMIPv6) [RFC5213] is the main network-based IP mobility protocol specified for IPv6. Proxy Mobile IPv4 [RFC5844] defines some IPv4 extensions. With network-based IP mobility protocols, the Local Mobility Anchor (LMA) typically provides the Anchoring Function (AF), Forwarding Management (FM) function, and Internetwork Location Information server (LIs) function. The mobile

access gateway (MAG) provides the Location Information client (LIC) function and Forwarding Management (FM) function to tunnel with LMA. PMIPv6 is architecturally almost identical to MIPv6, as the mobility signaling and routing between LMA and MAG in PMIPv6 is similar to those between HA and MN in MIPv6. The required mobility functionality at the MN is provided by the MAG so that the involvement in mobility support by the MN is not required.

We next describe some practices that show how network-based mobility protocols and several other protocol extensions can be deployed in a distributed mobility management environment.

One way to decentralize Proxy Mobile IPv6 operation can be to deploy several Local Mobility Anchors and use some selection criteria to assign LMAs to attaching mobile nodes. An example of this type of assignment is shown in Figure 4. As with the client based approach, a mobile node may use several anchors at the same time, each of them anchoring IP flows initiated at a different point of attachment. This assignment can be static or dynamic. The main advantage of this simple approach is that the IP address anchor, i.e., the LMA, could be placed closer to the mobile node. Therefore the resulting paths are close-to-optimal. On the other hand, as soon as the mobile node moves, the resulting path will start deviating from the optimal one.

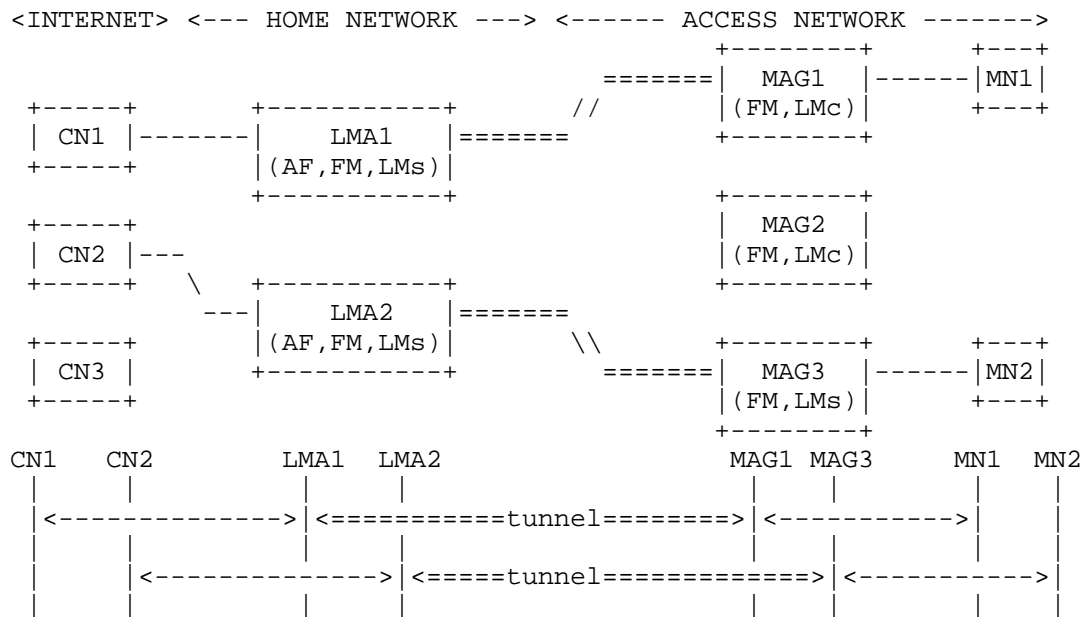


Figure 4: Distributed operation of Proxy Mobile IPv6

In a similar way to the host-based IP mobility case, network-based IP mobility has some extensions defined to mitigate the suboptimal routing issues that may arise due to the use of a centralized anchor. The Local Routing extensions [RFC6705] enable optimal routing in Proxy Mobile IPv6 in three cases: i) when two communicating MNs are attached to the same MAG and LMA, ii) when two communicating MNs are attached to different MAGs but to the same LMA, and iii) when two communicating MNs are attached to the same MAG but have different LMAs. In these three cases, data traffic between the two mobile nodes does not traverse the LMA(s), thus providing some form of path optimization since the traffic is locally routed at the edge. The main disadvantage of this approach is that it only tackles the MN-to-MN communication scenario, and only under certain circumstances.

An interesting extension that can also be used to facilitate the deployment of network-based mobility protocols in a distributed mobility management environment is the support of LMA runtime assignment described in [RFC6463]. This extension specifies a runtime Local Mobility Anchor assignment functionality and corresponding mobility options for Proxy Mobile IPv6. This runtime Local Mobility Anchor assignment takes place during the Proxy Binding Update / Proxy Binding Acknowledgment message exchange between a mobile access gateway and a local mobility anchor. While this mechanism is mainly aimed for load-balancing purposes, it can also be used to select an optimal LMA from the routing point of view. A runtime LMA assignment can be used to change the assigned LMA of an MN, for example, in cases when the mobile node does not have any active session, or when the running sessions can survive an IP address change. Note that several possible dynamic Local Mobility Anchor discovery solutions can be used, as described in [RFC6097].

#### 4.3. Flattening 3GPP mobile network approaches

The 3rd Generation Partnership Project (3GPP) is the standards development organization that specifies the 3rd generation mobile network and the Evolved Packet System (EPS) [SDO-3GPP.23.402], which mainly comprises the Evolved Packet Core (EPC) and a new radio access network, usually referred to as LTE (Long Term Evolution).

Architecturally, the 3GPP Evolved Packet Core (EPC) network is similar to an IP wireless network running PMIPv6 or MIPv6, as it relies on the Packet Data Network Gateway (PGW) anchoring services to provide mobile nodes with mobility support (see Figure 5). There are client-based and network-based mobility solutions in 3GPP, which for simplicity will be analyzed together. We next describe how 3GPP mobility protocols and several other completed or ongoing extensions can be deployed to meet some of the DMM requirements [RFC7333].

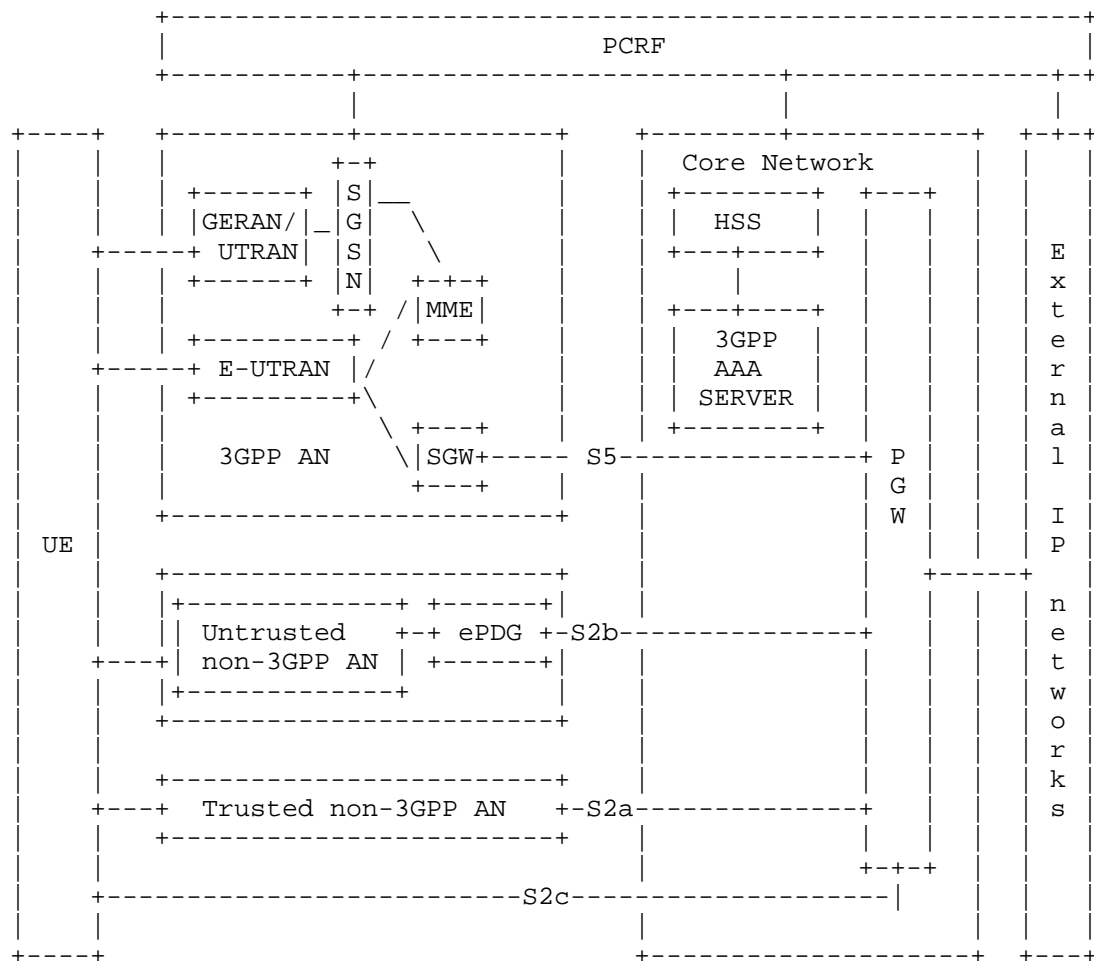


Figure 5: EPS (non-roaming) architecture overview

The GPRS Tunneling Protocol (GTP) [SDO-3GPP.29.060] [SDO-3GPP.29.281] [SDO-3GPP.29.274] is a network-based mobility protocol specified for 3GPP networks (S2a, S2b, S5 and S8 interfaces). In a similar way to PMIPv6, it can handle mobility without requiring the involvement of the mobile nodes. In this case, the mobile node functionality is provided in a proxy manner by the Serving Data Gateway (SGW), Evolved Packet Data Gateway (ePDG), or Trusted Wireless Access Gateway (TWAG [SDO-3GPP.23.402]).

3GPP specifications also include client-based mobility support, based on adopting the use of Dual-Stack Mobile IPv6 (DSMIPv6) [RFC5555] for the S2c interface [SDO-3GPP.24.303]. In this case, the User

Equipment (UE) implements the binding update functionality, while the home agent role is played by the PGW.

A Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) enabled network [SDO-3GPP.23.401] allows offloading some IP services at the local access network above the Radio Access Network (RAN) without the need to travel back to the PGW (see Figure 6).

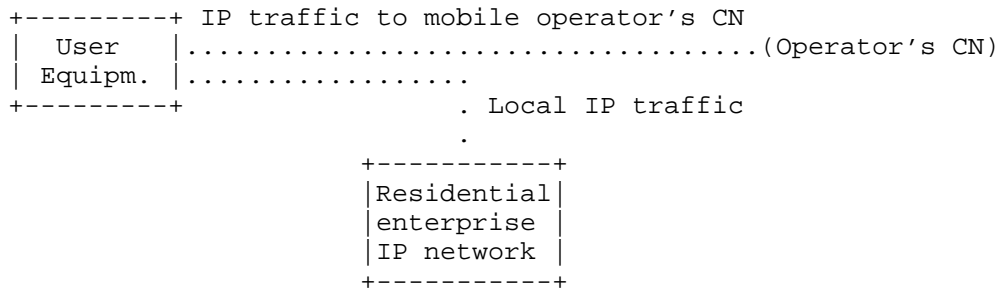


Figure 6: LIPA scenario

SIPTO enables an operator to offload certain types of traffic at a network node close to the UE's point of attachment to the access network, by selecting a set of GWs (SGW and PGW) that are geographically/topologically close to the UE's point of attachment.

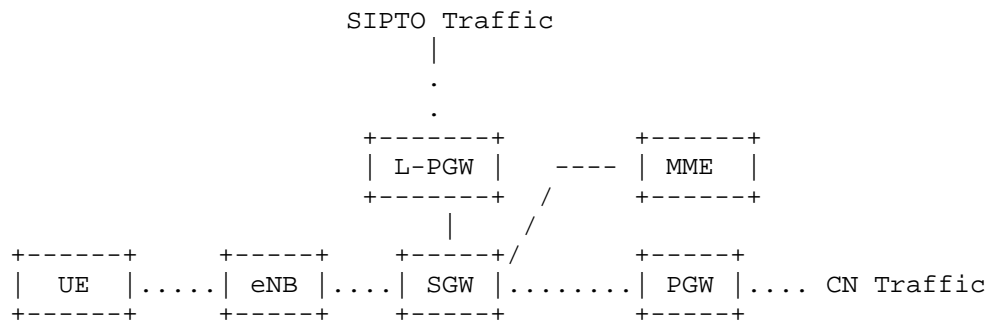


Figure 7: SIPTO architecture

LIPA, on the other hand, enables an IP addressable UE connected via a Home eNB (HeNB) to access other IP addressable entities in the same residential/enterprise IP network without traversing the mobile operator's network core in the user plane. In order to achieve this, a Local GW (LGW) collocated with the HeNB is used. LIPA is established by the UE requesting a new Public Data Network (PDN) connection to an access point name for which LIPA is permitted, and

the network selecting the Local GW associated with the HeNB and enabling a direct user plane path between the Local GW and the HeNB.

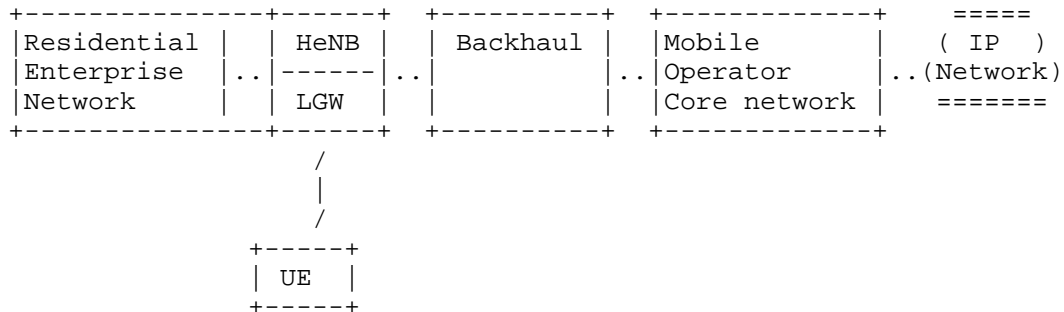


Figure 8: LIPA architecture

The 3GPP architecture specifications also provide mechanisms to allow discovery and selection of gateways [SDO-3GPP.29.303]. These mechanisms enable decisions taking into consideration topological location and gateway collocation aspects, relying upon the DNS as a "location database."

Both SIPTO and LIPA have a very limited mobility support, especially in 3GPP specifications up to Rel-12. Briefly, LIPA mobility support is limited to handovers between HeNBs that are managed by the same LGW (i.e., mobility within the local domain). There is no guarantee of IP session continuity for SIPTO.

## 5. Gap analysis

This section identifies the limitations in the current practices, described in Section 4, with respect to the DMM requirements listed in [RFC7333].

### 5.1. Distributed mobility management - REQ1

According to requirement REQ1 stated in [RFC7333], IP mobility, network access and forwarding solutions provided by DMM must make it possible for traffic to avoid traversing a single mobility anchor far from the optimal route.

From the analysis performed in Section 4, a DMM deployment can meet the requirement "REQ1 Distributed mobility management" usually relying on the following functions:

- o Multiple (distributed) anchoring: ability to anchor different sessions of a single mobile node at different anchors. In order



to provide improved routing, some anchors might need to be placed closer to the mobile node or the corresponding node.

- o Dynamic anchor assignment/re-location: ability to i) assign the initial anchor, and ii) dynamically change the initially assigned anchor and/or assign a new one (this may also require the transfer of mobility context between anchors). This can be achieved either by changing anchor for all ongoing sessions or by assigning new anchors just for new sessions.

GAP1-1: Both the main client- and network-based IP mobility protocols, namely (DS)MIPv6 and PMIPv6 allow deploying multiple anchors (i.e., home agents and localized mobility anchors), thereby providing the multiple anchoring function. However, existing solutions only provide an initial anchor assignment, thus the lack of dynamic anchor change/new anchor assignment is a gap. Neither the HA switch nor the LMA runtime assignment allows changing the anchor during an ongoing session. This actually comprises several gaps: ability to perform anchor assignment at any time (not only at the initial MN's attachment), ability of the current anchor to initiate/trigger the relocation, and ability to transfer registration context between anchors.

GAP1-2: Dynamic anchor assignment may lead the MN to manage different mobility sessions served by different mobility anchors. This is not an issue with client based mobility management where the mobility client natively knows the anchor associated with each of its mobility sessions. However, there is one gap, as the MN should be capable of handling IP addresses in a DMM-friendly way, meaning that the MN can perform smart source address selection (i.e., deprecating IP addresses from previous mobility anchors, so they are not used for new sessions). Besides, managing different mobility sessions served by different mobility anchors may raise issues with network based mobility management. In this case, the mobile client located in the network, e.g., MAG, usually retrieves the MN's anchor from the MN's policy profile as described in Section 6.2 of [RFC5213]. Currently, the MN's policy profile implicitly assumes a single serving anchor and thus does not maintain the association between home network prefix and anchor.

GAP1-3: The consequence of the distribution of the mobility anchors is that there might be more than one available anchor for a mobile node to use, which leads to an anchor discovery and selection issue. Currently, there is no efficient mechanism specified to allow the dynamic discovery of the presence of

nodes that can play the anchor role, discovering their capabilities and selecting the most suitable one. There is also no mechanism to allow selecting a node that is currently anchoring a given home address/prefix (capability sometimes required to meet REQ#2). However, there are some mechanisms that could help to discover anchors, such as the Dynamic Home Agent Address Discovery (DHAAD) [RFC6275], the use of the home agent flag (H) in Router Advertisements (which indicates that the router sending the Router Advertisement is also functioning as a Mobile IPv6 home agent on the link) or the MAP option in Router Advertisements defined by HMIPv6. Note that there are 3GPP mechanisms providing that functionality defined in [SDO-3GPP.29.303].

Regarding the ability to transfer registration context between anchors, there are already some solutions that could be reused or adapted to fill that gap, such as Fast Handovers for Mobile IPv6 [RFC5568] -- to enable traffic redirection from the old to the new anchor --, the Context Transfer protocol [RFC4067] -- to enable the required transfer of registration information between anchors --, or the Handover Keying architecture solutions [RFC6697], to speed up the re-authentication process after a change of anchor. Note that some extensions might be needed in the context of DMM, as these protocols were designed in the context of centralized client IP mobility, focusing on the access re-attachment and authentication.

GAP1-4: Also note that REQ1 is intended to prevent the data plane traffic from taking a suboptimal route. Distributed processing of the traffic may then be needed only in the data plane. Provision of this capability for distributed processing should not conflict with the use of a centralized control plane. Other control plane solutions such as charging, lawful interception, etc. should not be constrained by the DMM solution. On the other hand combining the control plane and data plane forwarding management (FM) function may limit the choice of solutions to those that distribute both data plane and control plane together. In order to enable distribution of only the data plane without distributing the control plane, it would be necessary to split the forwarding management function into the control plane (FM-CP) and data plane (FM-DP) components; there is currently a gap here.

## 5.2. Bypassable network-layer mobility support for each application session - REQ2

The requirement REQ2 for "bypassable network-layer mobility support for each application session" introduced in [RFC7333] requires flexibility in determining whether network-layer mobility support is needed. This requirement enables one to choose whether or not to use network-layer mobility support. The following two functions are also needed:

- o Dynamically assign/relocate anchor: a mobility anchor is assigned only to sessions which use the network-layer mobility support. The MN may thus manage more than one session; some of them may be associated with anchored IP address(es), while the others may be associated with local IP address(es).
- o Multiple IP address management: this function is related to the preceding and is about the ability of the mobile node to simultaneously use multiple IP addresses and select the best one (from an anchoring point of view) to use on a per-session/application/service basis. This requires MN to acquire information regarding the properties of the available IP addresses.

GAP2-1: The dynamic anchor assignment/relocation needs to ensure that IP address continuity is guaranteed for sessions that uses such mobility support (e.g., in some scenarios, the provision of mobility locally within a limited area might be enough from the mobile node or the application point of view) at the relocated anchor. Implicitly, when no applications are using the network-layer mobility support, DMM may release the needed resources. This may imply having the knowledge of which sessions at the mobile node are active and are using the mobility support. This is something typically known only by the MN, e.g., by its connection manager, and would also typically require some signaling support such as socket API extensions from applications to indicate to the IP stack whether mobility support is required or not. Therefore, (part of) this knowledge might need to be transferred to/shared with the network.

GAP2-2: Multiple IP address management provides the MN with the choice to pick the correct address, e.g., from those provided or not provided with mobility support, depending on the application requirements. When using client based mobility management, the mobile node is itself aware of the anchoring capabilities of its assigned IP addresses. This

is not necessarily the case with network based IP mobility management; current mechanisms do not allow the MN to be aware of the properties of its IP addresses. For example, the MN does not know whether the allocated IP addresses are anchored. However, there are proposals, such as [I-D.bhandari-dhc-class-based-prefix], [I-D.korhonen-6man-prefix-properties] and [I-D.anipko-mif-mpvd-arch] that the network could indicate such IP address properties during assignment procedures. Although these individual efforts exist and they could be considered as attempts to fix the gap, there is no solution adopted as a work item within any IETF working group.

GAP2-3: The handling of mobility management to the granularity of an individual session of a user/device needs proper session identification in addition to user/device identification.

### 5.3. IPv6 deployment - REQ3

This requirement states that DMM solutions should primarily target IPv6 as the primary deployment environment. IPv4 support is not considered mandatory and solutions should not be tailored specifically to support IPv4.

All analyzed DMM practices support IPv6. Some of them, such as MIPv6/NEMO including the support of dynamic HA selection, MOBIKE, SIPTO also have IPv4 support. Some solutions, e.g., PMIPv6, also have some limited IPv4 support. In conclusion, this requirement is met by existing DMM practices.

### 5.4. Considering existing mobility protocols - REQ4

A DMM solution must first consider reusing and extending IETF-standardized protocols before specifying new protocols.

As stated in [RFC7333], a DMM solution could reuse existing IETF and standardized protocols before specifying new protocols. Besides, Section 4 of this document discusses various ways to flatten and distribute current mobility solutions. Actually, nothing prevents the distribution of mobility functions within IP mobility protocols. However, as discussed in Section 5.1 and Section 5.2, limitations exist.

The 3GPP data plane anchoring function, i.e., the PGW, can also be distributed, but with limitations; e.g., no anchoring relocation, no context transfer between anchors and centralized control plane. The 3GPP architecture is also going in the direction of flattening with SIPTO and LIPA, though they do not provide full mobility support.

For example, mobility support for SIPTO traffic can be rather limited, and offloaded traffic cannot access operator services. Thus, the operator must be very careful in selecting which traffic to offload.

#### 5.5. Coexistence with deployed networks/hosts and operability across different networks - REQ5

According to [RFC7333], DMM implementations are required to co-exist with existing network deployments, end hosts and routers. Additionally, DMM solutions are expected to work across different networks, possibly operated as separate administrative domains, when the necessary mobility management signaling, forwarding, and network access are allowed by the trust relationship between them. All current mobility protocols can co-exist with existing network deployments and end hosts. There is no gap between existing mobility protocols and this requirement.

#### 5.6. Operation and management considerations - REQ6

This requirement actually comprises several aspects, as summarized below.

- o A DMM solution needs to consider configuring a device, monitoring the current operational state of a device, responding to events that impact the device, possibly by modifying the configuration and storing the data in a format that can be analyzed later.
- o A DMM solution has to describe in what environment and how it can be scalably deployed and managed.
- o A DMM solution has to support mechanisms to test if the DMM solution is working properly.
- o A DMM solution is expected to expose the operational state of DMM to the administrators of the DMM entities.
- o A DMM solution, which supports flow mobility, is also expected to support means to correlate the flow routing policies and the observed forwarding actions.
- o A DMM solution is expected to support mechanisms to check the liveness of the forwarding path.
- o A DMM solution has to provide fault management and monitoring mechanisms to manage situations where update of the mobility session or the data path fails.

- o A DMM solution is expected to be able to monitor the usage of the DMM protocol.
- o DMM solutions have to support standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules, which are expected to be created for DMM when needed for such configuration.

GAP6-1: Existing mobility management protocols have not thoroughly documented how, or whether, they support the above list of operation and management considerations. Each of the above needs to be considered from the beginning in a DMM solution.

GAP6-2: Management information base (MIB) objects are currently defined in [RFC4295] for MIPv6 and in [RFC6475] for PMIPv6. Standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules is lacking.

#### 5.7. Security considerations - REQ7

As stated in [RFC7333], a DMM solution has to support any security protocols and mechanisms needed to secure the network and to make continuous security improvements. In addition, with security taken into consideration early in the design, a DMM solution cannot introduce new security risks, or privacy concerns, or amplify existing security risks, that cannot be mitigated by existing security protocols and mechanisms.

Any solutions that are intended to fill in gaps identified in this document need to meet this requirement. At present, it does not appear that using existing solutions to support DMM has introduced any new security issues. For example, Mobile IPv6 defines security features to protect binding updates both to home agents and correspondent nodes. It also defines mechanisms to protect the data packets transmission for Mobile IPv6 users. Proxy Mobile IPv6 and other variations of mobile IP also have similar security considerations.

#### 5.8. Multicast - REQ8

It is stated in [RFC7333] that DMM solutions are expected to allow the development of multicast solutions to avoid network inefficiency in multicast traffic delivery.

Current IP mobility solutions address mainly the mobility problem for unicast traffic. Solutions relying on the use of an anchor point for tunneling multicast traffic down to the access router, or to the mobile node, introduce the so-called "tunnel convergence problem." This means that multiple instances of the same multicast traffic can

converge to the same node, diminishing the advantage of using multicast protocols.

[RFC6224] documents a baseline solution for the previous issue, and [RFC7028] a routing optimization solution. The baseline solution suggests deploying a Multicast Listener Discovery (MLD) proxy function at the MAG, and either a multicast router or another MLD proxy function at the LMA. The routing optimization solution describes an architecture where a dedicated multicast tree mobility anchor or a direct routing option can be used to avoid the tunnel convergence problem.

Besides the solutions highlighted before, there are no other mechanisms for mobility protocols to address the multicast tunnel convergence problem.

## 5.9. Summary

We next list the main gaps identified from the analysis performed above:

- GAP1-1: Existing solutions only provide an optimal initial anchor assignment, a gap being the lack of dynamic anchor change/new anchor assignment. Neither the HA switch nor the LMA runtime assignment allows changing the anchor during an ongoing session. MOBIKE allows change of GW but its applicability has been scoped to a very narrow use case.
- GAP1-2: The MN needs to be able to perform source address selection. Proper mechanism to inform the MN is lacking to provide the basis for the proper selection.
- GAP1-3: Currently, there is no efficient mechanism specified by the IETF that allows the dynamic discovery of the presence of nodes that can play the role of anchor, discover their capabilities and allow the selection of the most suitable one. However, the following mechanisms could help discovering anchors:
- Dynamic Home Agent Address Discovery (DHAAD): the use of the home agent (H) flag in Router Advertisements (which indicates that the router sending the Router Advertisement is also functioning as a Mobile IPv6 home agent on the link) and the MAP option in Router Advertisements defined by HMIPv6.
- GAP1-4: While existing network-based DMM practices may allow the deployment of multiple LMAs and dynamically select the best

one, this requires to still keep some centralization in the control plane, to access the policy database (as defined in RFC5213). Although [I-D.ietf-netext-pmip-cp-up-separation] allows a MAG to perform splitting of its control and user planes, there is a lack of solutions/extensions that support a clear control and data plane separation for IETF IP mobility protocols in a DMM context.

- GAP2-1: The information of which sessions at the mobile node are active and are using the mobility support need to be transferred to or shared with the network. Such mechanism has not been defined.
- GAP2-2: The mobile node needs to simultaneously use multiple IP addresses with different properties. There is a lack of mechanism to expose this information to the mobile node which can then update accordingly its source address selection mechanism.
- GAP2-3: The handling of mobility management has not been to the granularity of an individual session of a user/device before. The combination of session identification and user/device identification may be lacking.
- GAP6-1: Mobility management protocols have not thoroughly documented how, or whether, they support the following list of operation and management considerations:
- \* A DMM solution needs to consider configuring a device, monitoring the current operational state of a device, responding to events that impact the device, possibly by modifying the configuration and storing the data in a format that can be analyzed later.
  - \* A DMM solution has to describe in what environment and how it can be scalably deployed and managed.
  - \* A DMM solution has to support mechanisms to test if the DMM solution is working properly.
  - \* A DMM solution is expected to expose the operational state of DMM to the administrators of the DMM entities.
  - \* A DMM solution, which supports flow mobility, is also expected to support means to correlate the flow routing policies and the observed forwarding actions.



- \* A DMM solution is expected to support mechanisms to check the liveness of the forwarding path.
- \* A DMM solution has to provide fault management and monitoring mechanisms to manage situations where update of the mobility session or the data path fails.
- \* A DMM solution is expected to be able to monitor the usage of the DMM protocol.
- \* DMM solutions have to support standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules, which are expected to be created for DMM when needed for such configuration.

GAP6-2: Management information base (MIB) objects are currently defined in [RFC4295] for MIPv6 and in [RFC6475] for PMIPv6. Standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules is lacking.

## 6. Security Considerations

The deployment of DMM using existing IP mobility protocols raises similar security threats as those encountered in centralized mobility management systems. Without authentication, a malicious node could forge signaling messages and redirect traffic from its legitimate path. This would amount to a denial of service attack against the specific node or nodes for which the traffic is intended. Distributed mobility anchoring, while keeping current security mechanisms, might require more security associations to be managed by the mobility management entities, potentially leading to scalability and performance issues. Moreover, distributed mobility anchoring makes mobility security problems more complex, since traffic redirection requests might come from previously unconsidered origins, thus leading to distributed points of attack. Consequently, the DMM security design needs to account for the distribution of security associations between additional mobility entities and fulfill the security requirement of [RFC7333].

## 7. Contributors

This document has benefited to valuable contributions from

Charles E. Perkins  
Huawei Technologies  
EMail: charliep@computer.org

who had produced a matrix to compare the different mobility protocols and extensions against a list of desired DMM properties. They were useful inputs in the early work of gap analysis. He had continued to give suggestions as well as extensive review comments to this documents.

## 8. References

### 8.1. Normative References

- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC7333] Chan, H., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, August 2014.

### 8.2. Informative References

- [I-D.anipko-mif-mpvd-arch]  
Anipko, D., "Multiple Provisioning Domain Architecture", draft-anipko-mif-mpvd-arch-05 (work in progress), November 2013.
- [I-D.bhandari-dhc-class-based-prefix]  
Systems, C., Halwasia, G., Gundavelli, S., Deng, H., Thiebaut, L., Korhonen, J., and I. Farrer, "DHCPv6 class based prefix", draft-bhandari-dhc-class-based-prefix-05 (work in progress), July 2013.
- [I-D.gundavelli-v6ops-community-wifi-svcs]  
Gundavelli, S., Grayson, M., Seite, P., and Y. Lee, "Service Provider Wi-Fi Services Over Residential Architectures", draft-gundavelli-v6ops-community-wifi-svcs-06 (work in progress), April 2013.
- [I-D.ietf-netext-pmip-cp-up-separation]  
Wakikawa, R., Pazhyannur, R., Gundavelli, S., and C. Perkins, "Separation of Control and User Plane for Proxy Mobile IPv6", draft-ietf-netext-pmip-cp-up-separation-07 (work in progress), August 2014.
- [I-D.korhonen-6man-prefix-properties]  
Korhonen, J., Patil, B., Gundavelli, S., Seite, P., and D. Liu, "IPv6 Prefix Properties", draft-korhonen-6man-prefix-properties-02 (work in progress), July 2013.

- [IEEE.802-16.2009]  
"IEEE Standard for Local and metropolitan area networks  
Part 16: Air Interface for Broadband Wireless Access  
Systems", IEEE Standard 802.16, 2009,  
<[http://standards.ieee.org/getieee802/  
download/802.16-2009.pdf](http://standards.ieee.org/getieee802/download/802.16-2009.pdf)>.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P.  
Thubert, "Network Mobility (NEMO) Basic Support Protocol",  
RFC 3963, January 2005.
- [RFC4066] Liebsch, M., Singh, A., Chaskar, H., Funato, D., and E.  
Shim, "Candidate Access Router Discovery (CARD)", RFC  
4066, July 2005.
- [RFC4067] Loughney, J., Nakhjiri, M., Perkins, C., and R. Koodli,  
"Context Transfer Protocol (CXT)", RFC 4067, July 2005.
- [RFC4225] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E.  
Nordmark, "Mobile IP Version 6 Route Optimization Security  
Design Background", RFC 4225, December 2005.
- [RFC4295] Keeni, G., Koide, K., Nagami, K., and S. Gundavelli,  
"Mobile IPv6 Management Information Base", RFC 4295, April  
2006.
- [RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol  
(MOBIKE)", RFC 4555, June 2006.
- [RFC4640] Patel, A. and G. Giarretta, "Problem Statement for  
bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September  
2006.
- [RFC4889] Ng, C., Zhao, F., Watari, M., and P. Thubert, "Network  
Mobility Route Optimization Solution Space Analysis", RFC  
4889, July 2007.
- [RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC  
4960, September 2007.
- [RFC5014] Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6  
Socket API for Source Address Selection", RFC 5014,  
September 2007.
- [RFC5026] Giarretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6  
Bootstrapping in Split Scenario", RFC 5026, October 2007.

- [RFC5142] Haley, B., Devarapalli, V., Deng, H., and J. Kempf, "Mobility Header Home Agent Switch Message", RFC 5142, January 2008.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.
- [RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.
- [RFC5568] Koodli, R., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.
- [RFC6020] Bjorklund, M., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.
- [RFC6097] Korhonen, J. and V. Devarapalli, "Local Mobility Anchor (LMA) Discovery for Proxy Mobile IPv6", RFC 6097, February 2011.
- [RFC6224] Schmidt, T., Waehlich, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011.
- [RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.
- [RFC6463] Korhonen, J., Gundavelli, S., Yokota, H., and X. Cui, "Runtime Local Mobility Anchor (LMA) Assignment Support for Proxy Mobile IPv6", RFC 6463, February 2012.
- [RFC6475] Keeni, G., Koide, K., Gundavelli, S., and R. Wakikawa, "Proxy Mobile IPv6 Management Information Base", RFC 6475, May 2012.

- [RFC6611] Chowdhury, K. and A. Yegin, "Mobile IPv6 (MIPv6) Bootstrapping for the Integrated Scenario", RFC 6611, May 2012.
- [RFC6697] Zorn, G., Wu, Q., Taylor, T., Nir, Y., Hoeper, K., and S. Decugis, "Handover Keying (HOKEY) Architecture Design", RFC 6697, July 2012.
- [RFC6705] Krishnan, S., Koodli, R., Loureiro, P., Wu, Q., and A. Dutta, "Localized Routing for Proxy Mobile IPv6", RFC 6705, September 2012.
- [RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, September 2012.
- [RFC7028] Zuniga, JC., Contreras, LM., Bernardos, CJ., Jeon, S., and Y. Kim, "Multicast Mobility Routing Optimizations for Proxy Mobile IPv6", RFC 7028, September 2013.
- [SDO-3GPP.23.401]  
3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TS 23.401 10.10.0, March 2013.
- [SDO-3GPP.23.402]  
3GPP, "Architecture enhancements for non-3GPP accesses", 3GPP TS 23.402 10.8.0, September 2012.
- [SDO-3GPP.24.303]  
3GPP, "Mobility management based on Dual-Stack Mobile IPv6; Stage 3", 3GPP TS 24.303 10.0.0, June 2013.
- [SDO-3GPP.29.060]  
3GPP, "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface", 3GPP TS 29.060 3.19.0, March 2004.
- [SDO-3GPP.29.274]  
3GPP, "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3", 3GPP TS 29.274 10.11.0, June 2013.
- [SDO-3GPP.29.281]  
3GPP, "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)", 3GPP TS 29.281 10.3.0, September 2011.

[SDO-3GPP.29.303]

3GPP, "Domain Name System Procedures; Stage 3", 3GPP TS  
29.303 10.4.0, September 2012.

#### Authors' Addresses

Dapeng Liu (editor)  
China Mobile  
Unit2, 28 Xuanwumenxi Ave, Xuanwu District  
Beijing 100053  
China

Email: [liudapeng@chinamobile.com](mailto:liudapeng@chinamobile.com)

Juan Carlos Zuniga (editor)  
InterDigital Communications, LLC  
1000 Sherbrooke Street West, 10th floor  
Montreal, Quebec H3A 3G4  
Canada

Email: [JuanCarlos.Zuniga@InterDigital.com](mailto:JuanCarlos.Zuniga@InterDigital.com)  
URI: <http://www.InterDigital.com/>

Pierrick Seite  
Orange  
4, rue du Clos Courtel, BP 91226  
Cesson-Sevigne 35512  
France

Email: [pierrick.seite@orange.com](mailto:pierrick.seite@orange.com)

H Anthony Chan  
Huawei Technologies  
5340 Legacy Dr. Building 3  
Plano, TX 75024  
USA

Email: [h.a.chan@ieee.org](mailto:h.a.chan@ieee.org)

Carlos J. Bernardos  
Universidad Carlos III de Madrid  
Av. Universidad, 30  
Leganes, Madrid 28911  
Spain

Phone: +34 91624 6236  
Email: [cjbc@it.uc3m.es](mailto:cjbc@it.uc3m.es)  
URI: <http://www.it.uc3m.es/cjbc/>

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: December 7, 2014

H. Chan (Ed.)  
Huawei Technologies  
D. Liu  
China Mobile  
P. Seite  
Orange  
H. Yokota  
KDDI Lab  
J. Korhonen  
Broadcom Communications  
June 5, 2014

Requirements for Distributed Mobility Management  
draft-ietf-dmm-requirements-17

Abstract

This document defines the requirements for Distributed Mobility Management (DMM) at the network layer. The hierarchical structure in traditional wireless networks has led primarily to centrally deployed mobility anchors. As some wireless networks are evolving away from the hierarchical structure, it can be useful to have a distributed model for mobility management in which traffic does not need to traverse centrally deployed mobility anchors far from the optimal route. The motivation and the problems addressed by each requirement are also described.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."



This Internet-Draft will expire on December 7, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	4
2. Conventions used in this document . . . . .	5
2.1. Terminology . . . . .	5
3. Centralized versus distributed mobility management . . . . .	7
3.1. Centralized mobility management . . . . .	7
3.2. Distributed mobility management . . . . .	8
4. Problem Statement . . . . .	9
5. Requirements . . . . .	11
6. Security Considerations . . . . .	17
7. IANA Considerations . . . . .	17
8. Contributors . . . . .	17
9. References . . . . .	20
9.1. Normative References . . . . .	20
9.2. Informative References . . . . .	21
Authors' Addresses . . . . .	23

## 1. Introduction

In the past decade a fair number of network-layer mobility protocols have been standardized [RFC6275] [RFC5944] [RFC5380] [RFC6301] [RFC5213]. Although these protocols differ in terms of functions and associated message formats, they all employ a mobility anchor to allow a mobile node to remain reachable after it has moved to a different network. The anchor point, among other tasks, ensures connectivity by forwarding packets destined to, or sent from, the mobile node. It is a centrally deployed mobility anchor in the sense that the deployed architectures today have a small number of these anchors and the traffic of millions of mobile nodes in an operator network are typically managed by the same anchor. Such a mobility anchor may still have to reside in the subscriber's provider network even when the subscriber is roaming to a visited network, in order that certain functions such as charging and billing can be performed more readily by the provider's network. An example provider network is a Third Generation Partnership Project (3GPP) network.

Distributed mobility management (DMM) is an alternative to the above centralized deployment. The background behind the interests to study DMM are primarily in the following.

- (1) Mobile users are, more than ever, consuming Internet content including that of local Content Delivery Networks (CDNs). Such traffic imposes new requirements on mobile core networks for data traffic delivery. To prevent exceeding the available core network capacity, service providers need to implement new strategies such as selective IPv4 traffic offload (e.g., [RFC6909], 3GPP work items Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) [TS.23.401]) through alternative access networks such as Wireless Local Area Network (WLAN) [Paper-Mobile.Data.Offloading]. In addition, a gateway selection mechanism takes the user proximity into account within the Evolved Packet Core (EPC) [TS.29303]. Yet these mechanisms were not pursued in the past owing to charging and billing considerations which require solutions beyond the mobility protocol. Consequently, assigning a gateway anchor node from a visited network when roaming to the visited network has only recently been done and is limited to voice services.

Both traffic offloading and CDN mechanisms could benefit from the development of mobile architectures with fewer hierarchical levels introduced into the data path by the mobility management system. This trend of "flattening" the mobile networks works best for direct communications among peers in the same geographical area. Distributed mobility management in the flattening mobile networks would anchor the traffic closer to

the point of attachment of the user.

- (2) Today's mobile networks present service providers with new challenges. Mobility patterns indicate that mobile nodes often remain attached to the same point of attachment for considerable periods of time [Paper-Locating.User]. Specific IP mobility management support is not required for applications that launch and complete their sessions while the mobile node is connected to the same point of attachment. However, currently, IP mobility support is designed for always-on operation, maintaining all parameters of the context for each mobile subscriber for as long as they are connected to the network. This can result in a waste of resources and unnecessary costs for the service provider. Infrequent node mobility coupled with application intelligence suggest that mobility support could be provided selectively such as in [I-D.bhandari-dhc-class-based-prefix] and [I-D.korhonen-6man-prefix-properties], thus reducing the amount of context maintained in the network.

DMM may distribute the mobility anchors in the data-plane in flattening the mobility network such that the mobility anchors are positioned closer to the user; ideally, mobility agents could be collocated with the first-hop router. Facilitated by the distribution of mobility anchors, it may be possible to selectively use or not use mobility protocol support depending on whether such support is needed or not. It can thus reduce the amount of state information that must be maintained in various mobility agents of the mobile network. It can then avoid the unnecessary establishment of mechanisms to forward traffic from an old to a new mobility anchor.

This document compares distributed mobility management with centralized mobility management in Section 3. The problems that can be addressed with DMM are summarized in Section 4. The mandatory requirements as well as the optional requirements for network-layer distributed mobility management are given in Section 5. Finally, security considerations are discussed in Section 6.

The problem statement and the use cases [I-D.yokota-dmm-scenario] can be found in [Paper-Distributed.Mobility.Review].

## 2. Conventions used in this document

### 2.1. Terminology

All the general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275], in the Proxy mobile IPv6 specification

[RFC5213], and in Mobility Related Terminology [RFC3753]. These terms include the following: mobile node (MN), correspondent node (CN), and home agent (HA) as per [RFC6275]; local mobility anchor (LMA) and mobile access gateway (MAG) as per [RFC5213], and context as per [RFC3753].

In addition, this draft introduces the following terms.

#### Centrally deployed mobility anchors

refer to the mobility management deployments in which there are very few mobility anchors and the traffic of millions of mobile nodes in an operator network are managed by the same anchor.

#### Centralized mobility management

makes use of centrally deployed mobility anchors.

#### Distributed mobility management

is not centralized so that traffic does not need to traverse centrally deployed mobility anchors far from the optimal route.

#### Hierarchical mobile network

has a hierarchy of network elements arranged into multiple hierarchical levels which are introduced into the data path by the mobility management system.

#### Flattening mobile network

refers to the hierarchical mobile network which is going through the trend of reducing its number of hierarchical levels.

#### Flatter mobile network

has fewer hierarchical levels compared to a hierarchical mobile network.

#### Mobility context

is the collection of information required to provide mobility management support for a given mobile node.

### 3. Centralized versus distributed mobility management

Mobility management is needed because the IP address of a mobile node may change as the node moves. Mobility management functions may be implemented at different layers of the protocol stack. At the IP (network) layer, mobility management can be client-based or network-based.

An IP-layer mobility management protocol is typically based on the principle of distinguishing between a session identifier and a forwarding address and maintaining a mapping between the two. In Mobile IP, the new IP address of the mobile node after the node has moved is the forwarding address, whereas the original IP address before the mobile node moves serves as the session identifier. The location management (LM) information is kept by associating the forwarding address with the session identifier. Packets addressed to the session identifier will first route to the original network which re-directs them using the forwarding address to deliver to the session. Re-directing packets this way can result in long routes. An existing optimization routes directly using the forwarding address of the host, and such is a host-based solution.

The next two subsections explain centralized and distributed mobility management functions in the network.

#### 3.1. Centralized mobility management

In centralized mobility management, the location information in terms of a mapping between the session identifier and the forwarding address is kept at a single mobility anchor, and packets destined to the session identifier are forwarded via this anchor. In other words, such mobility management systems are centralized in both the control plane and the data plane (mobile node IP traffic).

Many existing mobility management deployments make use of centralized mobility anchoring in a hierarchical network architecture, as shown in Figure 1. Examples are the home agent (HA) and local mobility anchor (LMA) serving as the anchors for the mobile node (MN) and Mobile Access Gateway (MAG) in Mobile IPv6 [RFC6275] and in Proxy Mobile IPv6 [RFC5213] respectively. Cellular networks such as the 3GPP General Packet Radio System (GPRS) networks and 3GPP Evolved Packet System (EPS) networks employ centralized mobility management too. In the 3GPP GPRS network, the Gateway GPRS Support Node (GGSN), Serving GPRS Support Node (SGSN) and Radio Network Controller (RNC) constitute a hierarchy of anchors. In the 3GPP EPS network, the Packet Data Network Gateway (P-GW) and Serving Gateway (S-GW) constitute another hierarchy of anchors.

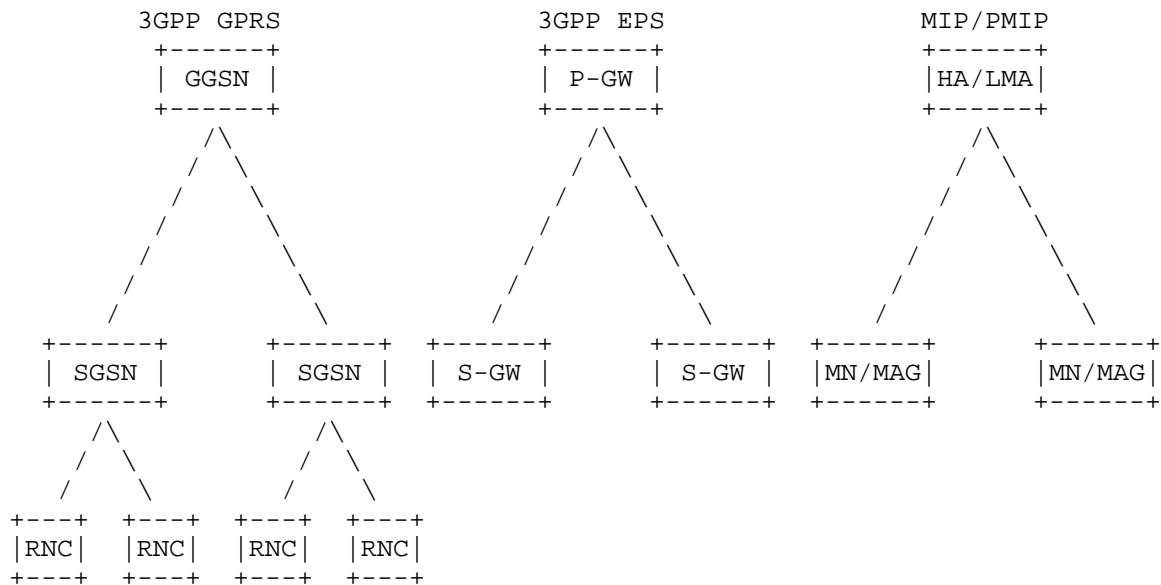


Figure 1. Centralized mobility management.

### 3.2. Distributed mobility management

Mobility management functions may also be distributed in the data plane to multiple networks as shown in Figure 2, so that a mobile node in any of these networks may be served by a nearby function with appropriate forwarding management (FM) capability.

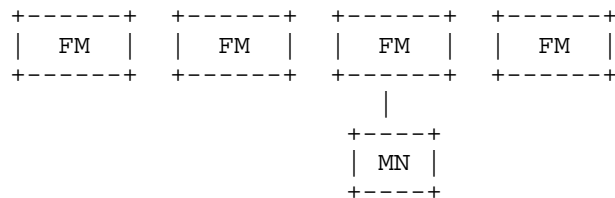


Figure 2. Distributed mobility management.

DMM is distributed in the data plane, whereas the control plane may either be centralized or distributed [I-D.yokota-dmm-scenario]. The former case implicitly assumes separation of data and control planes as described in [I-D.wakikawa-netext-pmip-cp-up-separation]. While mobility management can be distributed, it is not necessary for other functions such as subscription management, subscription database, and network access authentication to be similarly distributed.

A distributed mobility management scheme for a flattening mobile network consisting of access nodes is proposed in [Paper-Distributed.Dynamic.Mobility]. Its benefits over centralized mobility management have been shown through simulations [Paper-Distributed.Centralized.Mobility]. Moreover, the (re)use and extension of existing protocols in the design of both fully distributed mobility management [Paper-Migrating.Home.Agents] [Paper-Distributed.Mobility.SAE] and partially distributed mobility management [Paper-Distributed.Mobility.PMIP] [Paper-Distributed.Mobility.MIP] have been reported in the literature. Therefore, before designing new mobility management protocols for a future distributed architecture, it is recommended to first consider whether existing mobility management protocols can be extended.

#### 4. Problem Statement

The problems that can be addressed with DMM are summarized in the following:

PS1: Non-optimal routes

Forwarding via a centralized anchor often results in non-optimal routes, thereby increasing the end-to-end delay. The problem is manifested, for example, when accessing a nearby server or servers of a Content Delivery Network (CDN), or when receiving locally available IP multicast or sending IP multicast packets. (Existing route optimization is only a host-based solution. On the other hand, localized routing with PMIPv6 [RFC6705] addresses only a part of the problem where both the MN and the correspondent node (CN) are attached to the same MAG, and it is not applicable when the CN does not behave like an MN.)

PS2: Divergence from other evolutionary trends in network architectures such as distribution of content delivery.

Mobile networks have generally been evolving towards a flatter and flatter network. Centralized mobility management, which is non-optimal with a flatter network architecture, does not support this evolution.

PS3: Lack of scalability of centralized tunnel management and mobility context maintenance

Setting up tunnels through a central anchor and maintaining mobility context for each MN usually requires more concentrated resources in a centralized design, thus reducing scalability.



Distributing the tunnel maintenance function and the mobility context maintenance function among different network entities with proper signaling protocol design can avoid increasing the concentrated resources with an increasing number of MNs.

PS4: Single point of failure and attack

Centralized anchoring designs may be more vulnerable to single points of failures and attacks than a distributed system. The impact of a successful attack on a system with centralized mobility management can be far greater as well.

PS5: Unnecessary mobility support to clients that do not need it

IP mobility support is usually provided to all MNs. Yet it is not always required, and not every parameter of mobility context is always used. For example, some applications or nodes do not need a stable IP address during a handover to maintain session continuity. Sometimes, the entire application session runs while the MN does not change the point of attachment. Besides, some sessions, e.g., SIP-based sessions, can handle mobility at the application layer and hence do not need IP mobility support; it is then unnecessary to provide IP mobility support for such sessions.

PS6: Mobility signaling overhead with peer-to-peer communication

Wasting resources when mobility signaling (e.g., maintenance of the tunnel, keep alive signaling, etc.) is not turned off for peer-to-peer communication.

PS7: Deployment with multiple mobility solutions

There are already many variants and extensions of MIP as well mobility solutions at other layers. Deployment of new mobility management solutions can be challenging, and debugging difficult, when they co-exist with solutions already deployed in the field.

PS8: Duplicate multicast traffic

IP multicast distribution over architectures using IP mobility solutions (e.g., [RFC6224]) may lead to convergence of duplicated multicast subscriptions towards the downstream tunnel entity (e.g., MAG in PMIPv6). Concretely, when multicast subscription for individual mobile nodes is coupled with mobility tunnels (e.g., PMIPv6 tunnel), duplicate multicast subscription(s) is prone to be received through

different upstream paths. This problem may also exist or be more severe in a distributed mobility environment.

## 5. Requirements

After comparing distributed mobility management against centralized deployment in Section 3 and describing the problems in Section 4, this section identifies the following requirements:

### REQ1: Distributed mobility management

IP mobility, network access and forwarding solutions provided by DMM MUST enable traffic to avoid traversing single mobility anchor far from the optimal route.

This requirement on distribution is in the data plane only. It does not impose constraints on whether the control plane should be distributed or centralized. However, if the control plane is centralized while the data plane is distributed, it is implicit that the control plane and data plane need to separate (Section 3.2).

Motivation: This requirement is motivated by current trends in network evolution: (a) it is cost- and resource-effective to cache contents, and the caching (e.g., CDN) servers are distributed so that each user in any location can be close to one of the servers; (b) the significantly larger number of mobile nodes and flows call for improved scalability; (c) single points of failure are avoided in a distributed system; (d) threats against centrally deployed anchors, e.g., home agent and local mobility anchor, are mitigated in a distributed system.

This requirement addresses the problems PS1, PS2, PS3, and PS4 described in Section 4.

### REQ2: Bypassable network-layer mobility support for each application session

DMM solutions MUST enable network-layer mobility but it MUST be possible for any individual active application session (flow) to not use it. Mobility support is needed, for example, when a mobile host moves and an application cannot cope with a change in the IP address. Mobility support is also needed when a mobile router changes its IP address as it moves together with a host and, in the presence of ingress filtering, an application in the host is interrupted. However

mobility support at the network-layer is not always needed; a mobile node can often be stationary, and mobility support can also be provided at other layers. It is then not always necessary to maintain a stable IP address or prefix for an active application session.

Different active sessions can also differ in whether network-layer mobility support is needed. IP mobility, network access and forwarding solutions provided by DMM MUST then enable the possibility of independent handling for each application session of a user or mobile device.

The handling of mobility management to the granularity of an individual session of a user/device SHOULD need proper session identification in addition to user/device identification.

Motivation: The motivation of this requirement is to enable more efficient forwarding and more efficient use of network resources by selecting an IP address or prefix according to whether mobility support is needed and by not maintaining context at the mobility anchor when there is no such need.

This requirement addresses the problems PS5 and PS6 described in Section 4.

REQ3: IPv6 deployment

DMM solutions SHOULD target IPv6 as the primary deployment environment and SHOULD NOT be tailored specifically to support IPv4, in particular in situations where private IPv4 addresses and/or NATs are used.

Motivation: This requirement conforms to the general orientation of IETF work. DMM deployment is foreseen in mid-to long-term horizon, when IPv6 is expected to be far more common than today.

This requirement avoids the unnecessarily complexity in solving the problems in Section 4 for IPv4, which will not be able to use some of the IPv6-specific features.

REQ4: Existing mobility protocols

A DMM solution MUST first consider reusing and extending IETF-standardized protocols before specifying new protocols.

Motivation: Reuse of existing IETF work is more efficient and less error-prone.

This requirement attempts to avoid the need of new protocols development and therefore their potential problems of being time-consuming and error-prone.

- REQ5: Coexistence with deployed networks/hosts and operability across different networks

A DMM solution may require loose, tight or no integration into existing mobility protocols and host IP stack. Regardless of the integration level, DMM implementations MUST be able to coexist with existing network deployments, end hosts and routers that may or may not implement existing mobility protocols. Furthermore, a DMM solution SHOULD work across different networks, possibly operated as separate administrative domains, when the needed mobility management signaling, forwarding, and network access are allowed by the trust relationship between them.

Motivation: (a) to preserve backwards compatibility so that existing networks and hosts are not affected and continue to function as usual, and (b) enable inter-domain operation if desired.

This requirement addresses the problem PS7 described in Section 4.

- REQ6: Operation and Management considerations.

A DMM solution needs to consider configuring a device, monitoring the current operational state of a device, responding to events that impact the device, possibly by modifying the configuration and storing the data in a format that can be analyzed later. Different management protocols are available. For example:

- (a) SNMP [RFC1157] with definition of standardized management information base MIB objects for DMM, that allows monitoring traffic steering in a consistent manner across different devices,
- (b) NETCONF [RFC6241] with definition of standardized YANG [RFC6020] modules for DMM to achieve a standardized configuration,
- (c) syslog [RFC3164] which is a one-way protocol allowing a device to report significant events to a log analyzer in a network management system.

- (d) IP Flow Information Export (IPFIX) Protocol, which serves as a means for transmitting traffic flow information over the network [RFC7011], with a formal description of IPFIX Information Elements [RFC7012].

It is not the goal of the requirements document to impose which management protocol(s) should be used. An inventory of the management protocols and data models is covered in RFC 6632.

The following lists the operation and management considerations required for a DMM solution; the list may not be exhaustive and may be expanded according to the needs of the solutions:

A DMM solution **MUST** describe in what environment and how it can be scalably deployed and managed.

A DMM solution **MUST** support mechanisms to test if the DMM solution is working properly. For example, when a DMM solution employs traffic indirection to support a mobility session, implementations **MUST** support mechanisms to test that the appropriate traffic indirection operations are in place, including the setup of traffic indirection and the subsequent teardown of the indirection to release the associated network resources when the mobility session has closed.

A DMM solution **SHOULD** expose the operational state of DMM to the administrators of the DMM entities. For example, when a DMM solution employs separation between session identifier and forwarding address, it should expose the association between them.

When flow mobility is supported by a DMM solution, the solution **SHOULD** support means to correlate the flow routing policies and the observed forwarding actions.

A DMM solution **SHOULD** support mechanisms to check the liveness of forwarding path. If the DMM solution sends periodic update refresh messages to configure the forwarding path, the refresh period **SHOULD** be configurable and a reasonable default configuration value proposed. Information collected can be logged or made available with protocols such as SNMP [RFC1157], NETCONF [RFC6241], IPFIX [RFC7011], or syslog [RFC3164].

A DMM solution **MUST** provide fault management and monitoring

mechanisms to manage situations where update of the mobility session or the data path fails. The system must also be able to handle situations where a mobility anchor with ongoing mobility sessions fails.

A DMM solution SHOULD be able to monitor usage of DMM protocol. When a DMM solution uses an existing protocol, the techniques already defined for that protocol SHOULD be used to monitor the DMM operation. When these techniques are inadequate, new techniques MUST be developed.

In particular, the DMM solution SHOULD

- (a) be able to monitor the number of mobility sessions per user as well as their average duration.
- (b) provide indication on DMM performance such as
  - 1 the handover delay which includes the time necessary to re-establish the forwarding path when the point of attachment changes,
  - 2 the protocol reactivity which is the time between handover events such as the attachment to a new access point and the completion of the mobility session update.
- (c) provide means to measure the signaling cost of the DMM protocol.
- (d) if tunneling is used for traffic redirection, monitor
  - 1 the number of tunnels,
  - 2 their transmission and reception information,
  - 3 the used encapsulation method and overhead
  - 4 the security used at a node level.

DMM solutions SHOULD support standardized configuration with NETCONF [RFC6241], using YANG [RFC6020] modules, which SHOULD be created for DMM when needed for such configuration. However, if a DMM solution creates extensions to MIPv6 or PMIPv6, the allowed addition of the definition of management information base (MIB) objects to MIPv6 MIB [RFC4295] or PMIPv6 MIB [RFC6475] needed for the control and monitoring of

the protocol extensions SHOULD be limited to read-only objects.

Motivation: A DMM solution that is designed from the beginning for operability and manageability can avoid difficulty or incompatibility to implement efficient operations and management solutions.

These requirements avoid DMM designs that make operations and management difficult or costly.

REQ7: Security considerations

A DMM solution MUST support any security protocols and mechanisms needed to secure the network and to make continuous security improvements. In addition, with security taken into consideration early in the design, a DMM solution MUST NOT introduce new security risks, or amplify existing security risks, that cannot be mitigated by existing security protocols and mechanisms.

Motivation: Various attacks such as impersonation, denial of service, man-in-the-middle attacks, and so on, may be launched in a DMM deployment. For instance, an illegitimate node may attempt to access a network providing DMM. Another example is that a malicious node can forge a number of signaling messages thus redirecting traffic from its legitimate path. Consequently, the specific node or nodes to which the traffic is redirected may be under a denial of service attack, whereas other nodes do not receive their traffic. Accordingly, security mechanisms/protocols providing access control, integrity, authentication, authorization, confidentiality, etc. should be used to protect the DMM entities as they are already used to protect against existing networks and existing mobility protocols defined in IETF. Yet if a candidate DMM solution is such that even the proper use of these existing security mechanisms/protocols are unable to provide sufficient security protection, that candidate DMM solution is causing uncontrollable security problems.

This requirement prevents a DMM solution from introducing uncontrollable problems of potentially insecure mobility management protocols which make deployment infeasible because platforms conforming to the protocols are at risk for data loss and numerous other dangers, including financial harm to the users.

## REQ8: Multicast considerations

DMM SHOULD enable multicast solutions to be developed to avoid network inefficiency in multicast traffic delivery.

Motivation: Existing multicast deployment have been introduced after completing the design of the reference mobility protocol, often leading to network inefficiency and non-optimal forwarding for the multicast traffic. Instead DMM should consider multicast early so that the multicast solutions can better consider efficiency nature in the multicast traffic delivery (such as duplicate multicast subscriptions towards the downstream tunnel entities). The multicast solutions should then avoid restricting the management of all IP multicast traffic to a single host through a dedicated (tunnel) interface on multicast-capable access routers.

This requirement addresses the problems PS1 and PS8 described in Section 4.

## 6. Security Considerations

Please refer to the discussion under Security requirement in Section 5.

## 7. IANA Considerations

None

## 8. Contributors

This requirements document is a joint effort among numerous participants working in a team. Valuable comments and suggestions in various reviews from the following area directors and IESG members have also contributed to much improvements: Russ Housley, Catherine Meadows, Adrian Farrel, Barry Leiba, Alissa Cooper, Ted Lemon, Brian Haberman, Stephen Farrell, Joel Jaeggli, Alia Atlas, and Benoit Claise. In addition to the authors, each of the following has made very significant and important contributions to the working group draft in this work:

Charles E. Perkins  
Huawei Technologies  
Email: charliep@computer.org



Melia Telemaco  
Alcatel-Lucent Bell Labs  
Email: telemaco.melia@googlemail.com

Elena Demaria  
Telecom Italia  
via G. Reiss Romoli, 274, TORINO, 10148, Italy  
Email: elena.demaria@telecomitalia.it

Jong-Hyouk Lee  
Sangmyung University, Korea  
Email: jonghyouk@smu.ac.kr

Kostas Pentikousis  
EICT GmbH  
Email: k.pentikousis@eict.de

Tricci So  
ZTE  
Email: tso@zteusa.com

Carlos J. Bernardos  
Universidad Carlos III de Madrid  
Av. Universidad, 30, Leganes, Madrid 28911, Spain  
Email: cjbc@it.uc3m.es

Peter McCann  
Huawei Technologies  
Email: Peter.McCann@huawei.com

Seok Joo Koh  
Kyungpook National University, Korea  
Email: sjkoh@knu.ac.kr

Wen Luo  
ZTE  
No.68, Zijinhua RD,Yuhuatai District, Nanjing, Jiangsu 210012, China  
Email: luo.wen@zte.com.cn

Sri Gundavelli  
Cisco  
sgundave@cisco.com

Hui Deng  
China Mobile  
Email: denghui@chinamobile.com

Marco Liebsch

NEC Laboratories Europe  
Email: liebsch@neclab.eu

Carl Williams  
MCSR Labs  
Email: carlw@mcsr-labs.org

Seil Jeon  
Instituto de Telecomunicacoes, Aveiro  
Email: seiljeon@av.it.pt

Sergio Figueiredo  
Universidade de Aveiro  
Email: sfigueiredo@av.it.pt

Stig Venaas  
Email: stig@venaas.com

Luis Miguel Contreras Murillo  
Telefonica I+D  
Email: lmcm@tid.es

Juan Carlos Zuniga  
InterDigital  
Email: JuanCarlos.Zuniga@InterDigital.com

Alexandru Petrescu  
Email: alexandru.petrescu@gmail.com

Georgios Karagiannis  
University of Twente  
Email: g.karagiannis@utwente.nl

Julien Laganier  
Juniper  
Email: julien.ietf@gmail.com

Wassim Michel Haddad  
Ericsson  
Email: Wassim.Haddad@ericsson.com

Dirk von Hugo  
Deutsche Telekom Laboratories  
Email: Dirk.von-Hugo@telekom.de

Ahmad Muhanna  
Award Solutions  
Email: asmuhanna@yahoo.com

Byoung-Jo Kim  
ATT Labs  
Email: macsbug@research.att.com

Hassan Ali-Ahmad  
Orange  
Email: hassan.aliahmad@orange.com

Alper Yegin  
Samsung  
Email: alper.yegin@partner.samsung.com

David Harrington  
Effective Software  
Email: ietfdbh@comcast.net

## 9. References

### 9.1. Normative References

- [RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol (SNMP)", STD 15, RFC 1157, May 1990.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3164] Lonvick, C., "The BSD Syslog Protocol", RFC 3164, August 2001.
- [RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.
- [RFC4295] Keeni, G., Koide, K., Nagami, K., and S. Gundavelli, "Mobile IPv6 Management Information Base", RFC 4295, April 2006.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC6020] Bjorklund, M., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.
- [RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC6475] Keeni, G., Koide, K., Gundavelli, S., and R. Wakikawa, "Proxy Mobile IPv6 Management Information Base", RFC 6475, May 2012.
- [RFC6632] Ersue, M. and B. Claise, "An Overview of the IETF Network Management Standards", RFC 6632, June 2012.
- [RFC7011] Claise, B., Trammell, B., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, September 2013.
- [RFC7012] Claise, B. and B. Trammell, "Information Model for IP Flow Information Export (IPFIX)", RFC 7012, September 2013.

## 9.2. Informative References

- [I-D.bhandari-dhc-class-based-prefix]  
Bhandari, S., Halwasia, G., Gundavelli, S., Deng, H., Thiebaut, L., Korhonen, J., and I. Farrer, "DHCPv6 class based prefix", draft-bhandari-dhc-class-based-prefix-05 (work in progress), July 2013.
- [I-D.korhonen-6man-prefix-properties]  
Korhonen, J., Patil, B., Gundavelli, S., Seite, P., and D. Liu, "IPv6 Prefix Properties", draft-korhonen-6man-prefix-properties-02 (work in progress), July 2013.
- [I-D.wakikawa-netext-pmip-cp-up-separation]  
Wakikawa, R., Pazhyannur, R., Gundavelli, S., and C. Perkins, "Separation of Control and User Plane for Proxy Mobile IPv6", draft-wakikawa-netext-pmip-cp-up-separation-03 (work in progress), April 2014.
- [I-D.yokota-dmm-scenario]  
Yokota, H., Seite, P., Demaria, E., and Z. Cao, "Use case scenarios for Distributed Mobility Management", draft-yokota-dmm-scenario-00 (work in progress), October 2010.
- [Paper-Distributed.Centralized.Mobility]  
Bertin, P., Bonjour, S., and J-M. Bonnin, "A Distributed or Centralized Mobility", Proceedings of Global

Communications Conference (GlobeCom), December 2009.

[Paper-Distributed.Dynamic.Mobility]

Bertin, P., Bonjour, S., and J-M. Bonnin, "A Distributed Dynamic Mobility Management Scheme Designed for Flat IP Architectures", Proceedings of 3rd International Conference on New Technologies, Mobility and Security (NTMS), 2008.

[Paper-Distributed.Mobility.MIP]

Chan, H., "Distributed Mobility Management with Mobile IP", Proceedings of IEEE International Communication Conference (ICC) Workshop on Telecommunications: from Research to Standards, June 2012.

[Paper-Distributed.Mobility.PMIP]

Chan, H., "Proxy Mobile IP with Distributed Mobility Anchors", Proceedings of GlobeCom Workshop on Seamless Wireless Mobility, December 2010.

[Paper-Distributed.Mobility.Review]

Chan, H., Yokota, H., Xie, J., Seite, P., and D. Liu, "Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues", Journal of Communications, vol. 6, no. 1, pp. 4-15, February 2011.

[Paper-Distributed.Mobility.SAE]

Fisher, M., Anderson, F., Kopsel, A., Schafer, G., and M. Schlager, "A Distributed IP Mobility Approach for 3G SAE", Proceedings of the 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2008.

[Paper-Locating.User]

Kirby, G., "Locating the User", Communication International, 1995.

[Paper-Migrating.Home.Agents]

Wakikawa, R., Valadon, G., and J. Murai, "Migrating Home Agents Towards Internet-scale Mobility Deployments", Proceedings of the ACM 2nd CoNEXT Conference on Future Networking Technologies, December 2006.

[Paper-Mobile.Data.Offloading]

Lee, K., Lee, J., Yi, Y., Rhee, I., and S. Chong, "Mobile Data Offloading: How Much Can WiFi Deliver?", SIGCOMM 2010, 2010.

- [RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.
- [RFC5944] Perkins, C., "IP Mobility Support for IPv4, Revised", RFC 5944, November 2010.
- [RFC6224] Schmidt, T., Waehlich, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains", RFC 6224, April 2011.
- [RFC6301] Zhu, Z., Wakikawa, R., and L. Zhang, "A Survey of Mobility Support in the Internet", RFC 6301, July 2011.
- [RFC6705] Krishnan, S., Koodli, R., Loureiro, P., Wu, Q., and A. Dutta, "Localized Routing for Proxy Mobile IPv6", RFC 6705, September 2012.
- [RFC6909] Gundavelli, S., Zhou, X., Korhonen, J., Feige, G., and R. Koodli, "IPv4 Traffic Offload Selector Option for Proxy Mobile IPv6", RFC 6909, April 2013.
- [TS.23.401] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TR 23.401 10.10.0, March 2013.
- [TS.29303] 3GPP, "Domain Name System Procedures; Stage 3", 3GPP TR 23.303 11.2.0, September 2012.

#### Authors' Addresses

H Anthony Chan (editor)  
Huawei Technologies  
5340 Legacy Dr. Building 3, Plano, TX 75024, USA  
Email: h.a.chan@ieee.org

Dapeng Liu  
China Mobile  
Unit2, 28 Xuanwumenxi Ave, Xuanwu District, Beijing 100053, China  
Email: liudapeng@chinamobile.com

Pierrick Seite  
Orange  
4, rue du Clos Courtel, BP 91226, Cesson-Sevigne 35512, France  
Email: pierrick.seite@orange.com

Hidetoshi Yokota  
KDDI Lab  
2-1-15 Ohara, Fujimino, Saitama, 356-8502 Japan  
Email: yokota@kddilabs.jp

Jouni Korhonen  
Broadcom Communications  
Porkkalankatu 24, FIN-00180 Helsinki, Finland  
Email: jouni.nospam@gmail.com





DMM Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: August 18, 2014

M. Liebsch  
NEC  
P. Seite  
Orange-France Telecom  
G. Karagiannis  
University of Twente  
S. Gundavelli  
Cisco  
February 14, 2014

Distributed Mobility Management - Framework & Analysis  
draft-liebsch-dmm-framework-analysis-03.txt

Abstract

Mobile operators consider the distribution of mobility anchors to enable offloading some traffic from their core network. The Distributed Mobility Management (DMM) Working Group is investigating the impact of decentralized mobility management to existing protocol solutions, while taking into account well defined requirements, which are to be met by a future solution. This document discusses DMM using a functional framework. Functional Entities to support DMM as well as reference points between these Functional Entities are introduced and described. The described functional framework allows distribution and co-location of Functional Entities and build a DMM architecture that matches the architecture of available protocols. Such methodology eases the analysis of best current practices with regard to functional and protocol gaps.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 18, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Conventions and Terminology . . . . .	5
3. Functional Architecture for DMM Support . . . . .	6
4. Different Constellations of Functional Entities . . . . .	11
4.1. Condensed Deployment: Mobility Protocol Centric Solutions . . . . .	11
4.2. Cooperative Deployment: Distributed Architecture . . . . .	12
5. Security Considerations . . . . .	14
6. IANA Considerations . . . . .	15
7. References . . . . .	16
7.1. Normative References . . . . .	16
7.2. Informative References . . . . .	16
Appendix A. How the framework can support a gap analysis! Some examples.. . . .	17
A.1. Condensed Deployment using Mobile IPv6 . . . . .	17
A.2. Condensed Deployment using Proxy Mobile IPv6 . . . . .	17
A.3. Cooperative Deployment using LISP . . . . .	17
A.4. Cooperative Deployment using iBGP . . . . .	18
Appendix B. Functional Architecture for Multicast DMM Support . .	21
Appendix C. Change Notes . . . . .	25
Authors' Addresses . . . . .	26

## 1. Introduction

The concept of Distributed Mobility Management (DMM) is based on the distribution of mobility anchors towards the access networks to provide mobile nodes with local anchors and enable optimized routing of traffic above anchor level to any kind of serving point, e.g. distributed content caches. The closer mobility anchors are located to mobile nodes, the more a mobile node's handover may necessitate the assignment of a new mobility anchor. Continuity of a mobile node's IP address or IP address prefix enables IP session continuity, but creates the problem of routing downlink packets to the mobile node's current mobility anchor. Different solutions and associated extensions to IP mobility management protocols are being discussed to maintain a mobile node's IP session after mobility anchor relocation, including solutions that are based on existing protocols.

This document defines a functional framework for DMM and describes an initial set of well defined functional entities (FE), which are required to support IP address continuity in a network with distributed mobility anchors. Having identified the function of each FE as well as required interfaces between FEs allows different constellations of FEs, either by co-locating or distributing them. Functional frameworks have been successfully used within and outside of the IETF, such as the ITU-T [ITU-TY2018][ITU-TY2804], to support the thorough analysis of protocols gaps with existing protocols and to enable the design of suitable solutions. Due to the complexity of the DMM problem and solutions space, we consider such framework of particular importance for performing a Gap Analysis while assigning the defined FEs to architecture components of existing protocols and to build suitable solutions for DMM based on extensions to a single or multiple existing protocols and architecture components.

This version of the draft introduces a basic set of FEs and interfaces between these FEs to support IP address continuity in DMM, without being specific to the used mobility management protocol, which operates below the mobility anchor. The functional framework as per this draft is protocol agnostic, such that it can apply to (1) solutions that are solely based on existing IP mobility protocols and to (2) solutions which get support from non-mobility protocols.

The framework enables the analysis of existing protocols' suitability to support DMM and allows building optimized solutions for DMM without being limited to the mobility protocol suites. In particular, the framework can be used to build solutions on the following challenges that are currently being discussed in the context of DMM rechartering:

- o Support of different deployment models, where the mobility anchors can be located in the access networks or in the core/backbone network
- o Anchor selection mechanisms
- o Control- and Data-plane separation techniques for mobility components
- o Enhancements to mobile node for operating in a DMM-enabled network
- o Policy extensions for supporting DMM
- o Optimized traffic steering approaches for DMM used to ensure IP address continuity
- o Exposing mobility states (incl. binding state, access network parameters, etc.) to inter-work, for example, with SDN technology

Some examples how the framework can support the identification of required protocol extensions to existing mobility management protocol or alternatively the support from non-mobility protocols to design suitable DMM solutions on system level are described in Appendix A.

Appendix B defines an additional set of functional entities, which enables multicast support in DMM and can complement the framework for DMM unicast support.

## 2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

### 3. Functional Architecture for DMM Support

The framework introduces four additional functional entities (FE) which are relevant complement existing mobility- and transport networks to enable DMM support for unicast traffic and to meet essential DMM requirements as per [I-D.ietf-dmm-requirements], such as enabling temporary IP address continuity after a mobile node got assigned a new mobility anchor. Further FEs may be needed to enable advanced features, such as simultaneous use of an imported mobile node HoA or HNP to maintain ongoing data sessions and a new HoA or HNP, which is allocated by the mobile node's new mobility anchor after handover. Additional FEs are not considered in this revision of the draft, but can be introduced easily in future versions of the draft and considered for the BCP discussion and gap analysis.

The following FEs are currently considered as existing functional entities to build the mobility- and transport network:

- o FE\_R: Functional Entity of a standard IP Router / Switch
- o FE\_MA\_C: Functional Entity Mobility Anchor, Control Plane
- o FE\_MA\_U: Functional Entity Mobility Anchor, User Plane
- o FE\_MU\_C: Functional Entity Mobile User Client, Control Plane
- o FE\_MU\_U: Functional Entity Mobile User Client, User Plane

The list comprises a generic router/switch function FE\_R that's supposed to build the transport network. It has no particular function that's specific to DMM, but performs routing according to a longest prefix match. Deployment specific aspects, such as the use of IP/MPLS, are not (yet) considered in this draft.

The entities FE\_MA\_C and FE\_MA\_U represent the unmodified functions of the mobility architecture's mobility anchor. In Mobile IPv6, these function would be co-located with the Home Agent, in Proxy Mobile IPv6, these functions would be co-located with the Local Mobility Anchor (LMA). In a cellular IP (CIP) enabled domain, these functions would be co-located with the domain's CIP Gateway.

The entities FE\_MU\_C and FE\_MU\_U represent the existing user client functions, that send location updates to the mobility anchor. In Mobile IPv6, these functions are co-located with the Mobile Node, whereas in Proxy Mobile IPv6, these functions are co-located with the Mobile Access Gateway.

So far, this draft defines four DMM-specific FEs, which can be either

distributed or co-located with existing FEs of the mobility- or routing plane. One or more of the following FEs are currently assumed to add to an existing mobility- and transport network to enable DMM support for IP address continuity:

- o FE\_MCTX: Functional Entity Mobility Context Transfer
- o FE\_I: Functional Entity Ingress to DMM plane
- o FE\_E: Functional Entity Egress of DMM plane
- o FE\_IEC: Functional Entity for Ingress/Egress Control

Note: No all FEs or reference points between FEs may be relevant for a DMM-enabled solution that is based on existing protocols and the associated architecture. Which functions are relevant to complement an existing protocol and architecture depends on the identified gaps.

The task of the FE\_MCTX is to export relevant binding cache information, such as the mobile node's HoA or HNP, from the mobile node's previous mobility anchor (pMA) during mobility anchor relocation to enable IP address continuity after mobility anchor relocation. Furthermore, the function allows importing mobility context on the mobile node's new mobility anchor. Imported HoA/HNP of a mobile node will be treated as identifier and non-routable IP address (prefix), as it probably does not match the new mobility anchor's location in the topology. Furthermore, the FE\_MCTX can provide mobility context to the FE\_IEC to allow keeping these policies updated, which allow forwarding of packets to the MN's currently used mobility anchor.

The function FE\_I enables the ingress level of indirection by means of deviating from the standard routing path of the mobile node's downlink packets, which carry the mobile node's HoA/HNP in the destination IP address field of their IP header. The FE\_I can retrieve information from a control function (FE\_IEC) to establish forwarding of the mobile node's packets to the appropriate DMM egress function (FE\_E). Forwarding can be for example accomplished by an IP tunnel to the egress function, address translation to a routable IP address or other means.

The function FE\_E receives downlink packets being forwarded by the DMM ingress function FE\_I, e.g. by terminating a forwarding tunnel. The state on the FE\_I can be established through the DMM ingress/egress control function (FE\_IEC) and is used to identify an MN's received packets and deliver them to the MN's current mobility anchor (FE\_MA). If the FE\_E is co-located with the FE\_MA, the delivery is a local operation. If the FE\_E is not co-located with the FE\_MA, other

techniques, such as host-routes or technology such as OpenFlow may be used to deliver the packets to the mobile node's current mobility anchor. If not co-located with the FE\_MA, the FE\_E is supposed to be located close to the mobile node's current FE\_MA.

The function FE\_IEC represents a control function, that establishes, updates and removes policies (per-host or grouped) in the FE\_I and the FE\_E to allow forwarding of a mobile node's downlink packets towards the mobile node's current mobility anchor.

The mobile node's IP address (prefix) is carried in the source address field of the uplink packet. This source address is thus topologically incorrect after mobile node's handover. When IP routers of the mobility domain do not apply filtering according to the source addresses, uplink packets can be assumed to be routable and no specific operation is required.

If source address filtering is used, relevant routers need to be reconfigured to exclude the mobile node's IP address from filtering rules. If such filtering is performed by a mobility anchor or a Proxy Mobile IPv6 Mobile Access Gateway (MAG), local mobility functions on these routers should perform the task to reconfigure the local filter rules for uplink traffic.

When traffic indirection also applies to the uplink, e.g. to enable bidirectional tunneling to ensure that downlink and uplink data packets always traverse the same ingress/egress functions, FE\_E and FE\_I functions come into play on the uplink path. Downlink FE\_I and FE\_E become respectively FE\_E and FE\_I on the uplink. The uplink FE\_I forwards a mobile node's packets to the FE\_E corresponding to the downlink FE\_I that has sent packets with the mobile node's address in the destination address field. The FE\_I can also retrieve the information from the FE\_IEC.

Figure 1 illustrates how the four DMM-specific FEs complement existing FEs of the mobility architecture. These DMM-specific FEs and associated operation on the interfaces between them can be realized by existing protocols, extensions to them or new protocols. Figure 1 separates the data plane from the control plane.



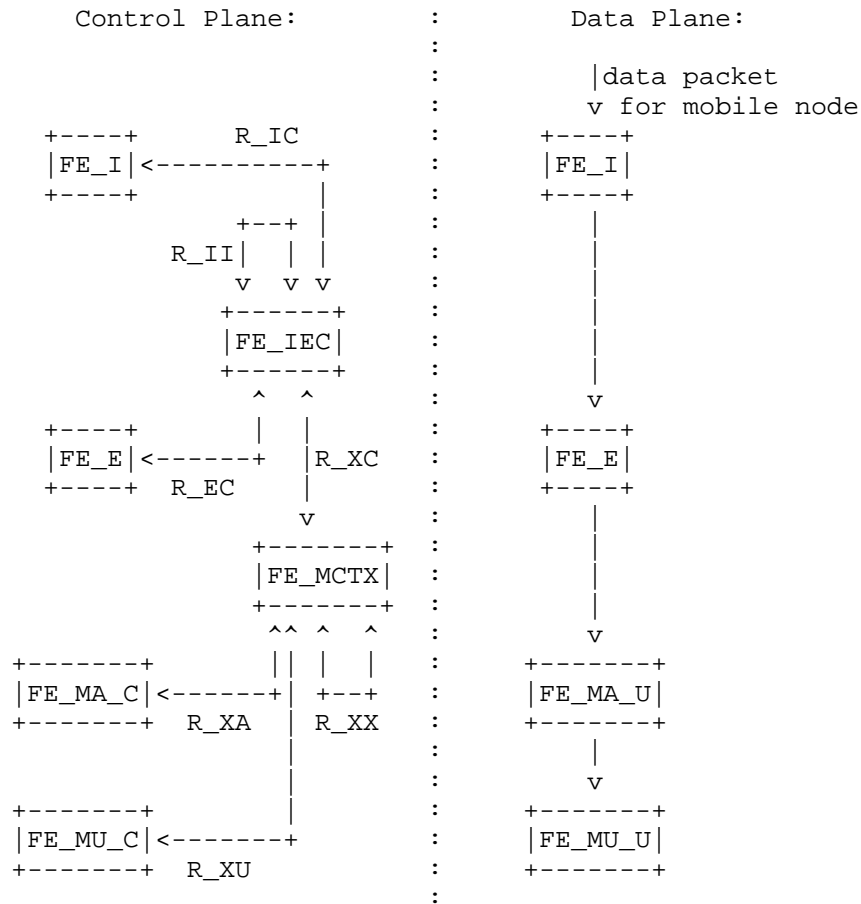


Figure 1: Basic set of functional entities (FE) and interfaces to enable IP-address continuity in DMM

The reference points between FEs comprise the following features:

- o R\_XA: Enables the FE\_MCTX to retrieve mobility context information from the FE\_MA of the MN's mobility anchor. Such information includes for example the MN's Home Address (HoA) or Home Network Prefix (HNP). In the network of the MN's new mobility anchor, the reference point enables the FE\_MCTX to provide the MN's mobility context to the associated FE\_MA, that imports the MN's mobility context to enable IP address continuity.
- o R\_XU: Enables the FE\_MCTX to retrieve mobility context information from the mobile user client control function, the FE\_MU\_C. In host

mobility management, this function is located on the Mobile Node, who could support DMM operation by notifying the FE\_MCTX through this reference point.

- o R\_XX: Enables the direct transfer of an MN's mobility context between two functions FE\_MCTX, which are typically located in the network of the MN's previous and new mobility anchor respectively.
- o R\_IC: Enables the FE\_IEC to provide policies to the FE\_I, which are used to forward the MN's downlink packets towards the MN's new mobility anchor and the associated FE\_E. These policies can be provided to the FE\_I in an unsolicited manner or on request by the FE\_I.
- o R\_EC: Enables the FE\_IEC to provide policies to the FE\_E, which are used at the FE\_E to identify received packets that belong to a particular MN and deliver these packets to the MN's new mobility anchor. Such policies could include, for example, tunnel endpoint information, flow identification rules or other identification and addressing rules.
- o R\_XC: Enables initialization and update of the FE\_IEC about the MN's mobility context as well as about its current location as represented by the FE\_E in the network of the MN's current mobility anchor.
- o R\_II: Multiple instances of an FE\_IEC can be deployed to build a DMM architecture, e.g. to distribute load and scale better, or distribute tasks associated with the FE\_IEC to enable cooperative solutions.

#### 4. Different Constellations of Functional Entities

The defined FEs can be grouped or distributed to build a DMM architecture that considers new architecture components or that is based on components of existing protocols. As a starting point, this section depicts and describes two deployment variants, which reflect the current understanding of the WG how DMM could be accomplished using existing protocol specifications as base. Variants of these two deployment models or entirely new models are possible and can be added to future versions of this document.

Note: This section is incomplete and needs further input on different deployment models and variants.

##### 4.1. Condensed Deployment: Mobility Protocol Centric Solutions

Mobility protocol centric solutions aim at extensions to available mobility protocols to enable DMM, without being dependent on any external, non-mobility component and protocol. IP address continuity is typically established on the control plane by extensions to the mobility protocol to convey an MN's mobility context to a new mobility anchor, and on the data plane by the establishment of a forwarding tunnel between mobility anchors to deliver downlink packets from the originally assigned mobility anchor to the MN's currently used mobility anchor after anchor relocation. Alternatively, IP address continuity is enabled by using multiple mobility anchors simultaneously, whereas the mobile node's IP address(es) remain anchored at the topologically correct anchor point. These approaches differ in the level of extensions to the mobility protocols and in the support of certain features on the mobile node, such as the simultaneous use of multiple mobility anchors and associated Home Addresses. They have in common the sub-optimal routing path, as the mobile node's downlink traffic needs to traverse the location of the IP addresses topologically correct mobility anchor.

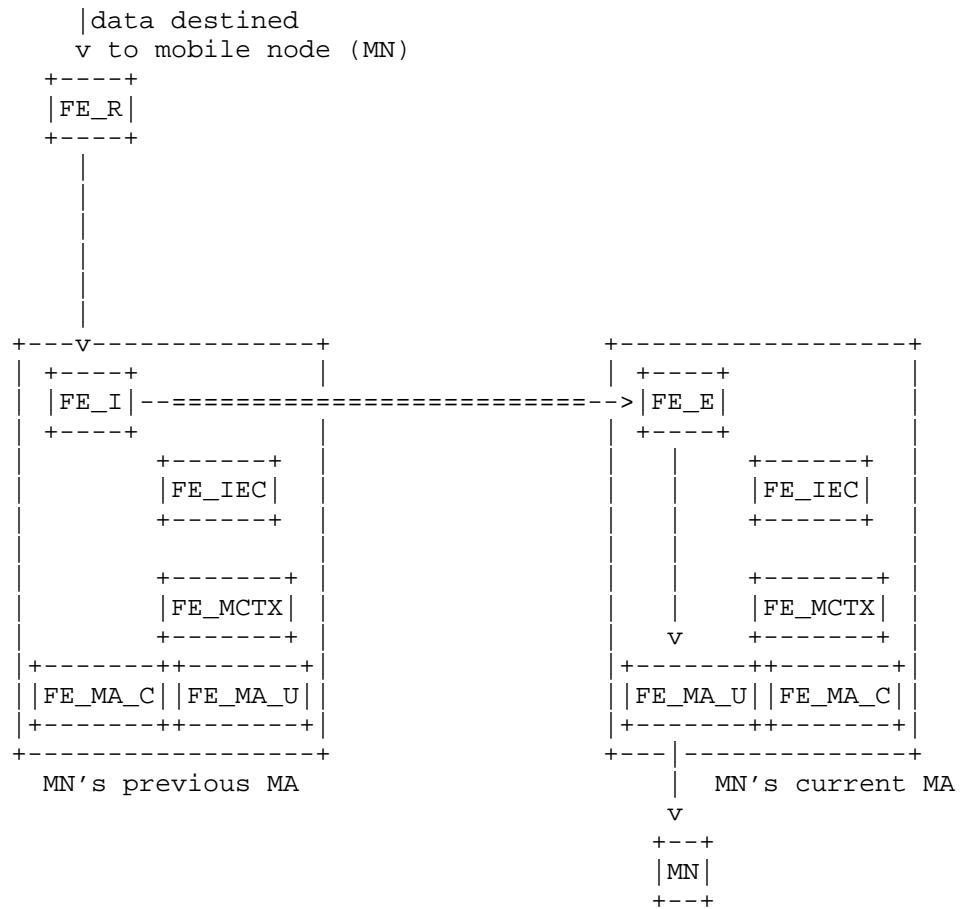


Figure 2: Condensed Deployment: Mobility Protocol Centric Solutions

#### 4.2. Cooperative Deployment: Distributed Architecture

A distributed architecture considers protocol operation between distributed FEs, aiming at a DMM solution that's to a large extent independent of the mobility architecture and protocol. A further goal is to establish optimal routing paths for the MN's traffic after the MN's mobility anchor has been relocated and IP address continuity must be provided.

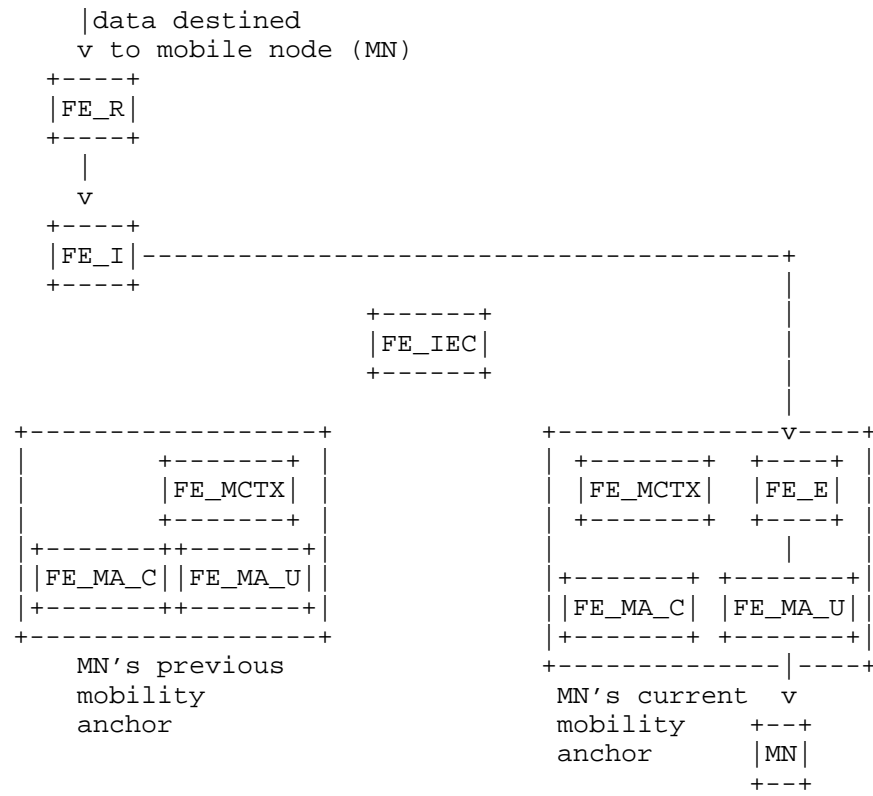


Figure 3: Cooperative Deployment: Distributed Architecture

## 5. Security Considerations

Different constellations of Functional Entities may allow re-use of existing protocols' security mechanisms to protect DMM protocol operation. In particular in a distributed model, new interfaces must be protected, e.g. to counteract unauthorized packet redirection to a different, possibly malicious mobility anchor. Details about security threats will be studied when the placement of Functional Entities for a selected set of preferred deployment models becomes mature.

## 6. IANA Considerations

As this document represents a framework and no protocol specification, there is no need for IANA actions.

## 7. References

### 7.1. Normative References

- [I-D.ietf-dmm-requirements]  
Chan, A., Liu, D., Seite, P., Yokota, H., and J. Korhonen,  
"Requirements for Distributed Mobility Management",  
draft-ietf-dmm-requirements-14 (work in progress),  
February 2014.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate  
Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas,  
"Protocol Independent Multicast - Sparse Mode (PIM-SM):  
Protocol Specification (Revised)", RFC 4601, August 2006.
- [RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick,  
"Internet Group Management Protocol (IGMP) / Multicast  
Listener Discovery (MLD)-Based Multicast Forwarding  
("IGMP/MLD Proxying")", RFC 4605, August 2006.
- [RFC6224] Schmidt, T., Waehlich, M., and S. Krishnan, "Base  
Deployment for Multicast Listener Support in Proxy Mobile  
IPv6 (PMIPv6) Domains", RFC 6224, April 2011.

### 7.2. Informative References

- [ITU-TY2018]  
"ITU-T Y.2018, Mobility management and control framework  
and architecture within the NGN transport stratum".
- [ITU-TY2804]  
"ITU-T Q.1707/Y.2804, Generic framework of mobility  
management for next generation networks".



## Appendix A. How the framework can support a gap analysis! Some examples..

A Gap analysis can be performed according to different deployment models and variants as summarized in Section 4. A suitable set of DMM FEs can be mapped to the architecture of existing protocols from within or beyond the IP mobility protocol solution space to analyze and identify gaps in the chosen protocols to support and optimize DMM operations. This section provides a few examples about the mapping of DMM FEs to mobility protocol FEs and non-mobility protocol FEs. Common goal is to enable DMM support, either in a mobility protocol centric manner or by means of a distributed architecture, relying on the support and associated collaboration with non-mobility protocol functions, such as routing. As examples for the distributed architecture, the Locator-Identifier Split Protocol (LISP) and the iBGP have been used to enable traffic indirection in the routing plane above the topological level of distributed mobility anchors.

### A.1. Condensed Deployment using Mobile IPv6

Note: A detailed example needs to be added in a next revision.

Description: Framework mapping to existing Mobile IPv6 architecture. Technical approach is the establishment of a forwarding tunnel between previous HA and new HA to enable IP address continuity after anchor relocation. Approach is the identification of missing protocol functions in Mobile IPv6 as expected from DMM functional entities as per this specification to enable full DMM support.

### A.2. Condensed Deployment using Proxy Mobile IPv6

Note: A detailed example needs to be added in a next revision.

Description: Framework mapping to existing Proxy Mobile IPv6 architecture. Technical approach is the establishment of a forwarding tunnel between previous LMA and new LMA to enable IP address continuity after anchor relocation. Approach is the identification of missing protocol functions in Proxy Mobile IPv6 as expected from DMM functional entities as per this specification to enable full DMM support.

### A.3. Cooperative Deployment using LISP

This example utilizes LISP Tunnel Ingress Routers (TIR) to perform the LISP map and encap procedure and tunnel packets to the mobile node's current mobility anchor (Figure 4). The mobile node's IP address is assumed routable above TIR level. TIRs can be for example deployed close to a mobile operator's IXP or close to operator-owned

traffic sources, such as a mobile Content Delivery Network (CDN). A TIR, which receives data packets destined to the mobile node, can consult the LISP Mapping Database (DB) to resolve the mobile node's IP address into its current locator, which is the mobile node's currently used mobility anchor. The mobility anchor has to terminate the LISP tunnel at the Tunnel Egress Router (TER) function and forward the data packets to the mobile node's current location according to the utilized mobility management protocol. An identified gap in a setup with LISP is the dynamic update of the Mapping Database and the update of already established states in TIRs in case the mobile node's location has changed from one mobility anchor to another mobility anchor.

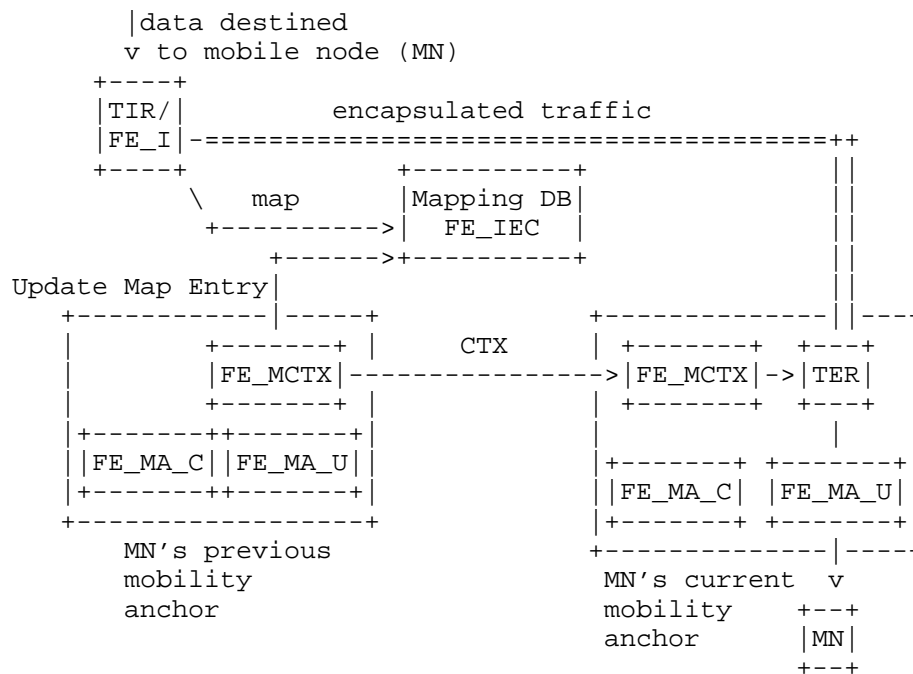


Figure 4: Example: DMM indirection at LISP TIRs

#### A.4. Cooperative Deployment using iBGP

This example utilizes the iBGP to establish per-host or group states in iBGP routers and forward a mobile node's packets hop-by-hop to its currently used mobility anchor. Figure 5 depicts an iBGP router with co-located FE\_E and FE\_I to receive data packets and to forward these packets to the next hop according to the routing state as per iBGP

update. The FE\_IEC can be represented by the iBGP component to enable the setup of distributed routing states in distributed iBGP routers to direct the mobile node's data packets to its current mobility anchor. Hence, the FE\_IEC is distributed in all iBGP routers to collaborate in the setup of host routes. The mobility anchor itself must implement iBGP to contribute to the distribution and update of host routes, e.g. after the mobile node changed its mobility anchor while IP address continuity must be supported. Since iBGP has been designed to propagate routing states to distributed routers, only minor protocol gaps may be identified in a detailed analysis. Beyond protocol gaps, further aspects need to be analyzed in such setup, which include limitations in scalability and route update latency.

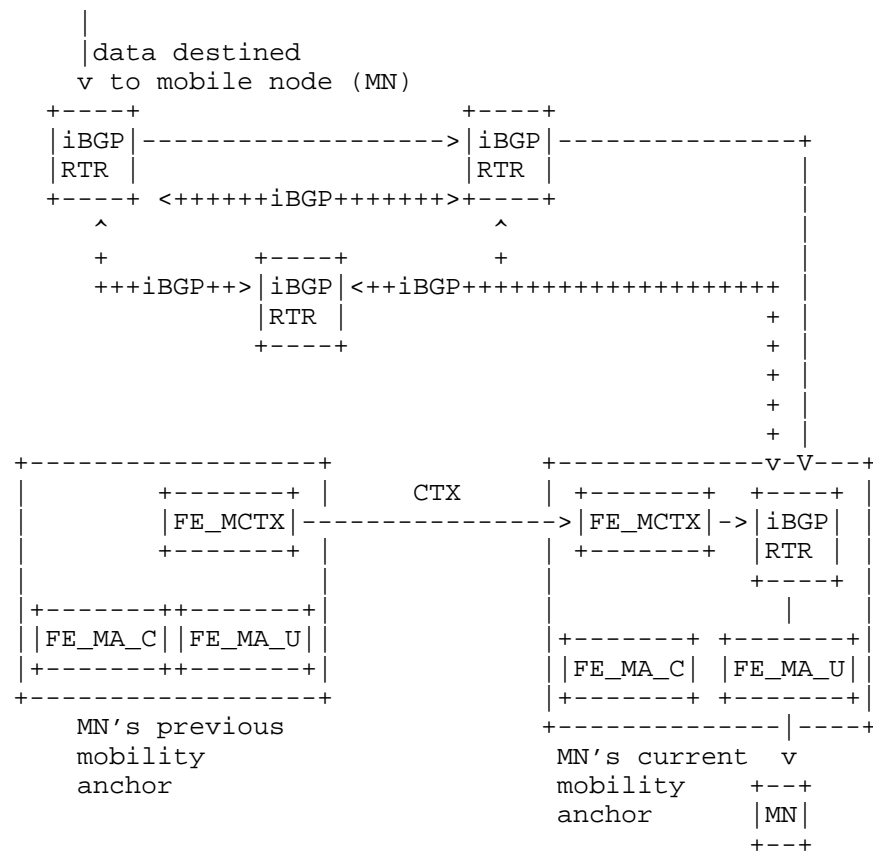
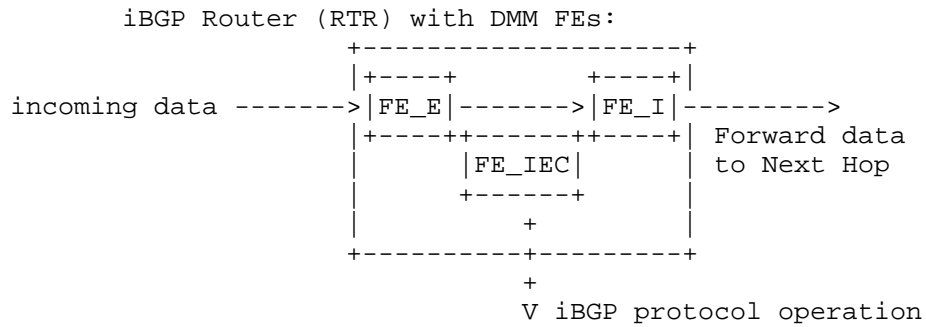


Figure 5: Example: DMM indirection at iBGP routers

## Appendix B. Functional Architecture for Multicast DMM Support

The framework for multicast DMM support is similar to the framework for unicast DMM support introduced in Section 3 with the main difference that the additional introduced features are needed to support the multicast control and user plane. This framework, similar to the one introduced in Section 3, introduces four DMM-specific, with the main difference that these FEs are able to support multicast traffic, instead of unicast traffic. Additional FEs might be needed but are not considered in this revision of the draft, but can be introduced easily in future versions of the draft and considered for the BCP discussion and gap analysis.

The following FEs are currently considered as existing multicast based Functional entities to build the mobility- and transport network:

- o FE\_MR: Functional Entity of a standard Multicast IP Router / Switch. This FE can be incorporated to support the functionality of a Rendezvous Point (RP) and of a Designated Router (DR), see e.g., [RFC4601].
- o FE\_MLD-P: Functional Entity of a standard Multicast Listener Discovery Proxy (MLSD-P) used to provide MLD based forwarding, following the operation defined in e.g., [RFC4605] and [RFC6224].
- o FE\_MA\_C\_M: Functional Entity Mobility Anchor, Control Plane, for the support of multicast traffic
- o FE\_MA\_U\_M: Functional Entity Mobility Anchor, User Plane, for the support of multicast traffic
- o FE\_MU\_C: Functional Entity Mobile User Client, Control Plane, for the support of unicast and multicast traffic. In case of multicast traffic the FE\_MU\_C can operate as multicast sender and multicast listener.
- o FE\_MU\_U: Functional Entity Mobile User Client, User Plane, for the support of unicast and multicast traffic. In case of multicast traffic the FE\_MU\_U can operate as multicast sender and multicast listener.

The four DMM-specific FEs used to support multicast traffic are listed below.

- o FE\_MCTX\_M: Functional Entity Mobility Context Transfer, used for the support of multicast traffic.

- o FE\_I\_M: Functional Entity Ingress to DMM plane, used for the support of multicast traffic.
- o FE\_E\_M: Functional Entity Egress of DMM plane, used for the support of multicast traffic.
- o FE\_IEC\_M: Functional Entity for Ingress/Egress Control, used for the support of multicast traffic.

These FEs support similar features as the ones supported by the FE\_MCTX, FE\_I, FE\_E, FE\_IEC FEs, respectively, described in Section 3, with the main difference that they are used for the support of the multicast control and user planes, instead of the unicast control and user planes.

Figure 6 depicts the basic set of functional entities (FE) and interfaces to enable IP-address continuity in multicast based DMM. The four DMM-specific FEs and their associated operation on the interfaces between them can be realized by existing protocols, extensions to them or new protocols.

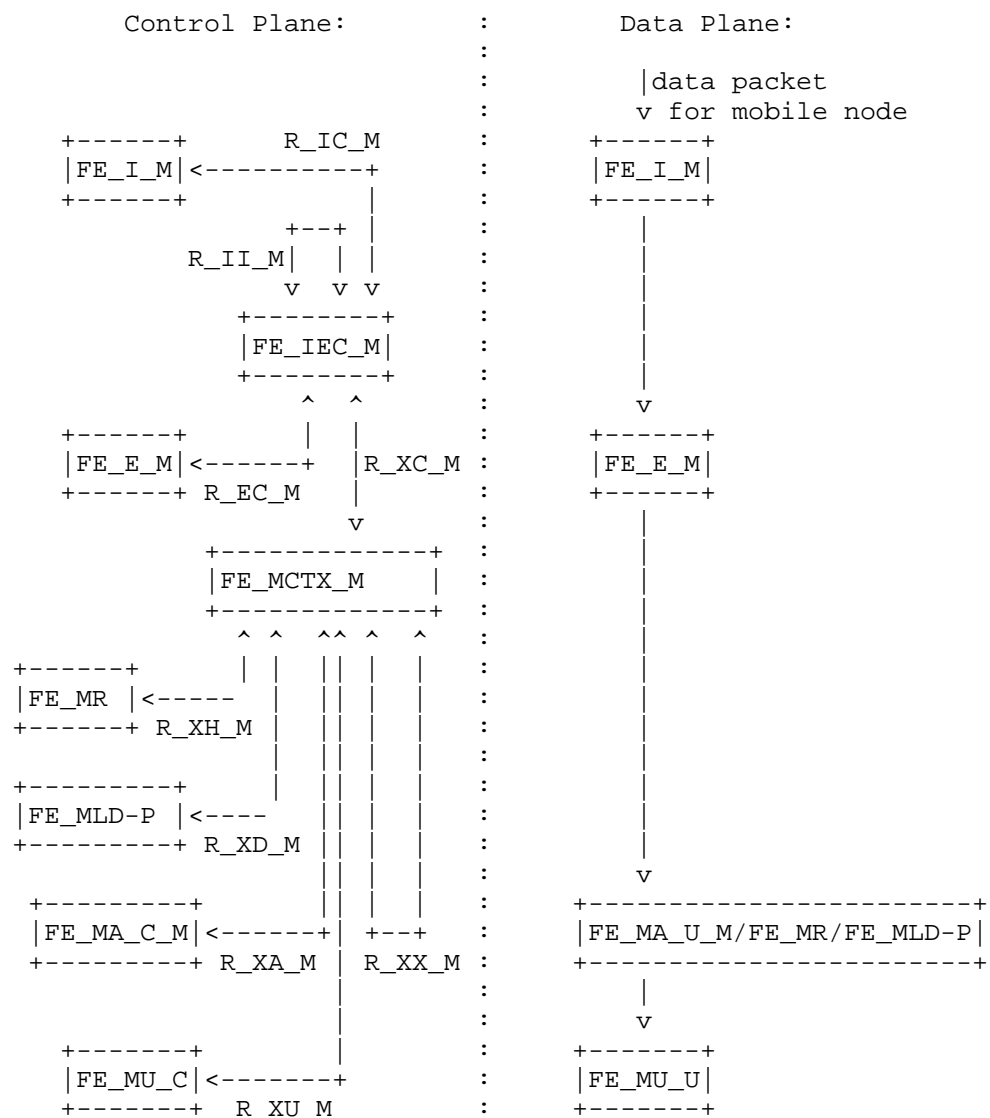


Figure 6: Basic set of functional entities (FE) and interfaces to enable IP-address continuity in multicast based DMM

The reference points between FEs are shown in Figure 6. In particular the features comprised by the reference points R\_XA\_M, R\_XU\_M, R\_XX\_M, R\_IC\_M, R\_EC\_M, R\_XC\_M, R\_II\_M, are similar to the ones supported by the reference points R\_XA, R\_XU, R\_XX, R\_IC, R\_EC, R\_XC, R\_II, respectively, described in Section 3, with the difference that they are used to support the multicast based control plane,

instead of supporting the unicast based control plane.

Two additional reference points are added that are comprising the following features:

- o R\_XH\_M: Enables the FE\_MCTX\_M to retrieve MR routing based information from FE\_MR following the operation defined in e.g., [RFC4601].
- o R\_XD\_M: Enables the FE\_MCTX\_M to retrieve Multicast Listener Discovery forwarding information from FE\_MLD-P following the operation defined in e.g., [RFC4605] and [RFC6224].



## Appendix C. Change Notes

Changes in version 01:

- o Introduced functional split between existing Mobility Anchor Control- and User-Plane
- o Introduced functional split of existing mobile user client Control- and User-Plane
- o Added uplink routing considerations in DMM architecture
- o Description of a first DMM Multicast framework in the Appendix
- o Added examples to the appendix about how to use the framework for a gap analysis and for the design of optimized DMM solutions

Authors' Addresses

Marco Liebsch  
NEC Laboratories Europe  
NEC Europe Ltd.  
Kurfuersten-Anlage 36  
D-69115 Heidelberg,  
Germany

Phone: +49 6221 4342146  
Email: liebsch@neclab.eu

Pierrick Seite  
Orange-France Telecom  
4, rue du Clos Courtel, BP 91226  
Cesson-Sevigne, 35512  
France

Phone:  
Email: pierrick.seite@orange-ftgroup.com

Georgios Karagiannis  
University of Twente  
AE Enschede, 7500  
Netherlands

Phone: +31 53 4894099  
Email: karagian@cs.utwente.nl

Sri Gundavelli  
Cisco  
170 West Tasman Drive  
San Jose, CA 95134  
USA

Email: sgundave@cisco.com



Network Working Group  
Internet Draft  
Intended status: Informational  
Expires: March 27, 2014

M. Liu  
Y. Wang  
ICT, CAS  
September 27, 2013

Distributed Mobility Management: Service Flows Distribution and  
Handoff Technique based on MIPv6  
draft-liu-dmm-flows-distribution-and-handoff-01

## Abstract

This document has a normative description of the service flow management technology based on mobile IPv6 (MIPv6). It makes the upgrade of management model in MIPv6 from the entire node granularity to the single service flow granularity. It proposes a distributed mobility management solution, DMIPv6, which is compatible with MIPv6 and takes different mobility management strategies according to the Correspondent Node's position, network conditions and service requirements of different service flows so as to achieve the service flow handoff and transmission path control. The standard also provides route optimization mechanism between the Mobile Node and the ordinary Correspondent Node that doesn't support mobile IPv6.

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on March 27, 2014.

## Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction .....	2
2. Conventions used in this document .....	3
2.1. Conventions used in this document .....	3
2.2. Terminology .....	3
3. Basic Framework .....	4
4. Message Types .....	5
4.1. Messages Between MN and HA .....	6
4.2. Messages Between MN and CN .....	6
4.3. DHP Query Message .....	6
4.4. DHoA Request/Response Message .....	13
4.5. DHP Binding Update/Confirmation Message .....	15
5. DMIPv6 Workflow .....	17
5.1. The Processing Workflow of New Service Connection .....	17
5.2. The Processing Workflow when MN Moves .....	20
6. Security Considerations .....	21
7. IANA Considerations .....	21
8. References .....	22
8.1. Normative References .....	22
8.2. Informative References .....	22
Authors' Addresses .....	23

## 1. Introduction

This standard proposes a distributed mobility management protocol, DMIPv6, which is compatible with the standard mobile IPv6 protocol. DMIPv6 introduces Distributed Home-Proxy (DHP) and Distributed Home

Address (DHoA) for a Mobile Node (MN) while there are Home Agent (HA) and Home-Of-Address (HoA) already. MN will use DMIPv6 proposed in this document if the DHP and DHoA are available, otherwise the standard mobile IPv6 is used. The deployment of the DMIPv6 could be implemented step by step, with the compatibility to the existing mobile IPv6.

What's more, compared to the standard mobile IPv6 in management model, DMIPv6 could select different DHP for a MN's different service flows. MN takes different management strategy for different service flows according to network conditions and the actual requirements during the move. The introduction of DHP not only reduces the home network congestion and HA load, but also greatly reduces the possible failures in home network and HA, and the bad impacts to the MN. Besides, the MN could achieve optimized transmission path and transmission delay even choosing bidirectional tunnel, because the DHP is located close to the Correspondent Node (CN). For CN that is a server, the introduction of DHP makes it possible for it to enhance its mobility support for its clients without any updates of itself.

## 2. Conventions and Terminology

### 2.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119].

### 2.2. Terminology

All general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobility Support in IPv6 specification [RFC6275] and in the Proxy mobile IPv6 specification [RFC5213]. These terms include mobile node (MN), correspondent node (CN), home agent (HA), Care-of-Address (CoA), Home-of-Address (HoA), Binding Update (BU), and Binding Acknowledgement (BA).

In addition, this document uses the following terms:

Distributed Home-Proxy (DHP) is a router near CN, with the function for an extension of the HA, which assigns distributed home address for the MN, receives and forwards the packet between the MN and CN. It plays a role in router optimization and handoff management on service flow granularity.

Distributed Mobile IPv6 (DMIPv6) is a distributed network layer mobility solution compatible with mobile IPv6, which would take different mobility management strategies according to the CN's position, network conditions and service requirements of different service flows so as to achieve the service flow handoff and transmission path control. And the standard will also provide route optimization mechanism between the MN and the ordinary CN that doesn't support mobile IPv6.

Distributed Home Address (DHoA) is a home address that MN gets from the corresponding DHP for establishing a connection with CN so as to achieve the service flow handoff and transmission path control.

### 3. Basic Framework

Distributed Mobile IPv6(DMIPv6), which is a distributed mobility management architecture compatible with Mobile IPv6, introduces Distributed Home-Proxy(DHP) to the existing Mobile IPv6 architecture. In DMIPv6, DHP can be deployed in subdomain of each network.

DHP is implemented based on HA, and multiple DHPs independent of each other can be deployed in the same domain. The DHP is deployed the same style as the HA and general router. Under such condition, MN can select one or more DHPs according to the state of DHP and service demand. In general, one DHP is enough, but multiple DHPs can be selected to backup or improve concurrent performance. Figure 1 shows the basic architecture of DMIPv6:

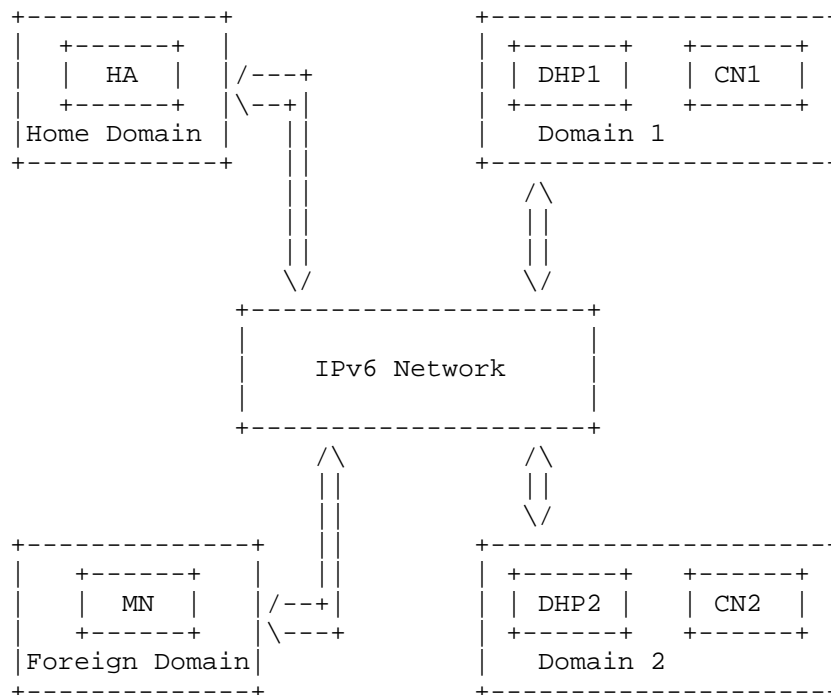


Figure 1 Architecture of Service Flow Distribution and Handoff

#### Management

As Figure 1, there exists multiple independent DHPs in the CN network, and MN can select one of them as the proxy server. The introduction of DHP greatly decreases the MN's dependence on HA, and can also optimize the transmission path and transmission delay.

When MN moves to a new link, the DHP can act as a proxy and forward the data for it. According to the deployment style and the available equipment's support to DMIPv6, MN will perform DMPv6 if the DHP and DHoA are available, otherwise the standard mobile IPv6 is used.

#### 4. Message Types

In this standard, majority of equipments need to complete a series of interactions to transmit information. The following messages are extended from the standard ICMPv6 messages. All extension types of the extended ICMP messages are different from those of standards defined by international organizations like IETF. If collisions occur in the future, values of corresponding message types should be adjusted according to the actual situation.



#### 4.1. Messages Between MN and HA

Messages between MN and HA include binding update message (BU) sent when MN moves and binding acknowledgment messages (BA). This standard is compatible with standard mobile IPv6 protocol. For detailed information about the above messages, refer to the IETF RFC 6275.

#### 4.2. Messages Between MN and CN

Messages between MN and CN include binding update message (BU) sent when MN updates its CoA-address and binding acknowledgment messages (BA). This standard is compatible with standard mobile IPv6 protocol. For detailed information about the above messages, refer to the IETF RFC 6275.

#### 4.3. DHP Query Message

DHP query message is used by MN to perform the DHP query and selection operations. This standard proposes 3 kinds of DHP query method. Corresponding query methods are depicted as follow:

##### 4.3.1. Dynamic DHP Discovery Query/Acknowledgement Message

In this method, DHP query messages are sent to corresponding network to request response directly. This procedure is similar to "dynamic home agent address discovery mechanism" in MIPv6. When adopt this method, all DHPs in a common CN domain should maintain the status information of other DHPs, i.e. every DHP maintains a list of information about all DHPs in current domain.

When comes to specific operation, MN query the DNS to get the DHP anycast address in the CN domain, and then send dynamic DHP discovery query message to that anycast address. According to the routing protocols, the topologically nearest DHP from the mobile node may receive the request message and then respond to it. Status information of all DHPs in the CN domain should be included in the reply message. MN can perform the HP selection based on this state information. This approach is the active query mode of MN.

## 4.3.1.1. DHP Query Message

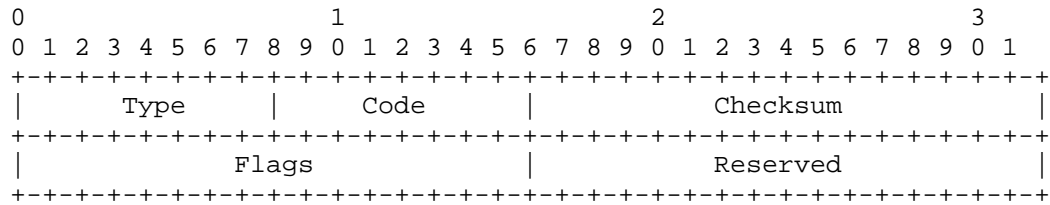


Figure 2 Dynamic DHP Discovery Query Message

- o Source address: IPv6 address of the interface sending this message
- o Destination address: anycast address of DHP in the CN domain
- o Hop limit: 255
- o Authentication Header: sender should contain this header field when security association of IP authentication header present between sender and receiver.
- o ICMP fields:
  - Type 160
  - Code 0
  - Checksum ICMP checksum
  - Reserved Reserved for future use. The value must be initialized to zero by the sender, and must be ignored by the receiver.

## 4.3.1.2. DHP Acknowledgement Message

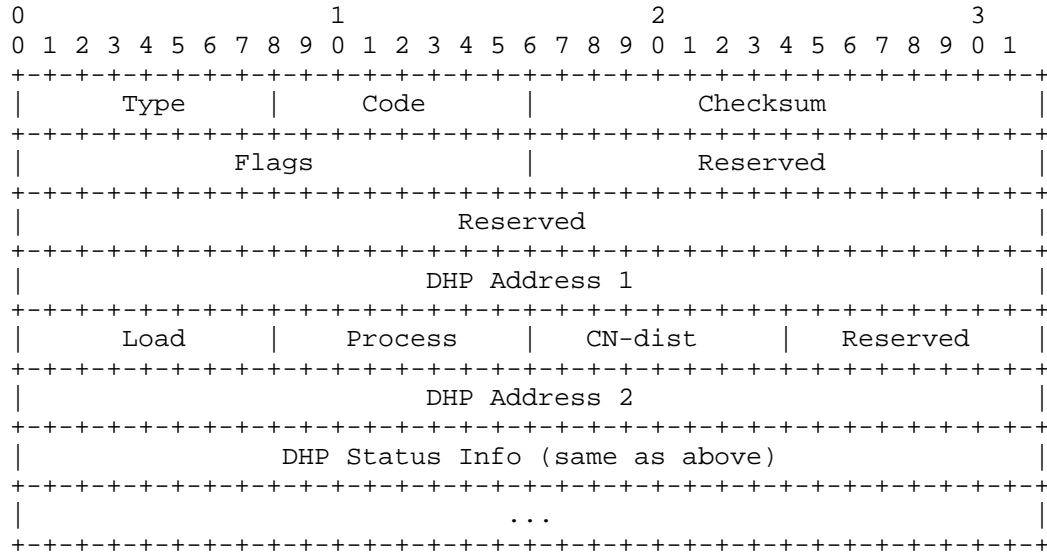


Figure 3 Dynamic DHP Discovery Acknowledgement Message

- o Source address: IPv6 address of the interface sending this message
- o Destination address: IPv6 address of MN
- o Hop limit: 255
- o Authentication Header: sender should contain this header field when security association of IP authentication header present between sender and receiver. Source address: IPv6 address of the interface sending this message
- o ICMP fields:

Type 161

Code 0

Checksum ICMP checksum

Reserved Reserved for future use. The value must be initialized to zero by the sender, and must be ignored by the receiver.

- o Options: Sender must contain following options in the request message:

DHP proxy server address: local IPv6 address of the sender. This address should be a DHP network interface address. If there exists more than one DHP in current network domain, information of all DHPs should be sequentially contained in the options part.

DHP status information: the current DHP state information should include load conditions, process capability, distance from CN and so on.

#### 4.3.2. Multicast Request DHP Query/Acknowledgement Message

Through this method, IP address and status information of DHP in the CN domain can be obtained by sending multicast request message. This method requires all DHPs from one CN domain form a multicast group, then share a multicast address.

Firstly MN query the DNS to get the DHP multicast address in the CN domain, and then send query message to that multicast address. Since then, all DHPs in the multicast group will reply acknowledgement message to the MN which also contains DHP address and other status information. This also is a MN active query method.

##### 4.3.2.1. DHP Query Message

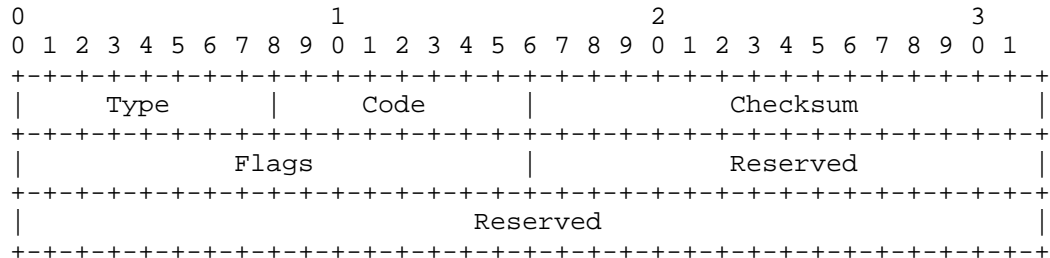


Figure 4 Multicast Request DHP Query Message

- o Source address: IPv6 address of the interface sending this message
- o Destination address: DHP multicast address in the CN domain
- o Hop limit: 255

- o Authentication Header: sender should contain this header field when security association of IP authentication header present between sender and receiver.

- o ICMP fields:

Type 162

Code 0

Checksum ICMP checksum

Reserved Reserved for future use. The value must be initialized to zero by the sender, and must be ignored by the receiver.

#### 4.3.2.2. DHP Acknowledgement Message

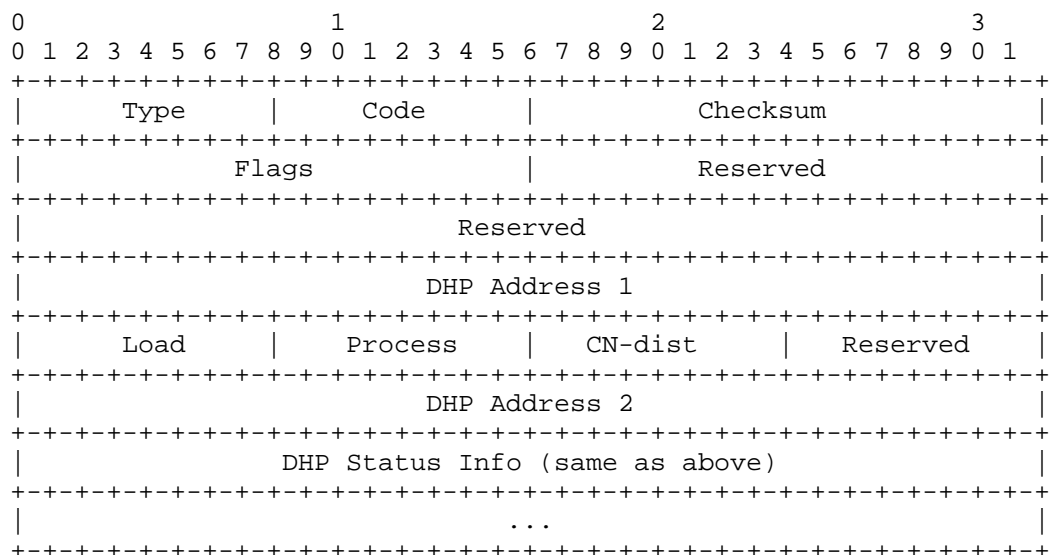


Figure 5 Multicast Request DHP Acknowledgement Message

- o Source address: IPv6 address of the interface sending this message
- o Destination address: IPv6 address of MN
- o Hop limit: 255

- o Authentication Header: sender should contain this header field when security association of IP authentication header present between sender and receiver.

- o ICMP fields:

Type 163

Code 0

Checksum ICMP checksum

Reserved Reserved for future use. The value must be initialized to zero by the sender, and must be ignored by the receiver.

- o Options: Sender must contain following options in the request message:

DHP proxy server address: local IPv6 address of the sender.

DHP status information: state information of this machine, contains load conditions, process capability, distance from CN and so on.

The distance here is as same as defined above. Depending on the routing protocols, it may be the number of hops or delay in the actual network topology.

#### 4.3.3. Specific Server DHP Query/Response Message

The DHP selection can also use special DHP management server to complete. In actual circumstances, we can set global DHP management server to maintain all the DHP status information in the real-time network.

MN can use DNS to query the DHP management server's address, and then send the corresponding DHP query messages to the server, the server sends the request a timely response.

In accordance with different handling ways of MN, these methods can be divided into two categories: active and passive queries.

##### 4.3.3.1. Active Query

In this way, the MN sends a request message to DHP management server, the server will send all of the information to the MN terminal, for MN itself to make a choice. It is called MN active query.

## 4.3.3.1.1. DHP query message

The DHP query message in this way is the same with the corresponding query message in 4.3.1, the difference is that the message type code is 164 and the destination address is DHP management server address.

## 4.3.3.1.2. DHP Query Response Message

DHP query response message in this way is the same with the corresponding query response message in 4.3.1, the difference is that the message type code is 165 and the destination address is DHP management server address.

## 4.3.3.2. Passive Query

Different from the above mentioned active query, in the passive way, the MN sends a request message to the DHP information management server, the request message further includes business type that MN initiate currently and other relevant requirements of DHP ( including the ability to handle, the size of the load, the routing hops requests and so on. According to the requirements of MN, DHP information management server complete DHP preferred choice for MN in predetermined rules , then the selected DHP information response to MN. The Message format is as below:

## 4.3.3.2.1. DHP Query Message

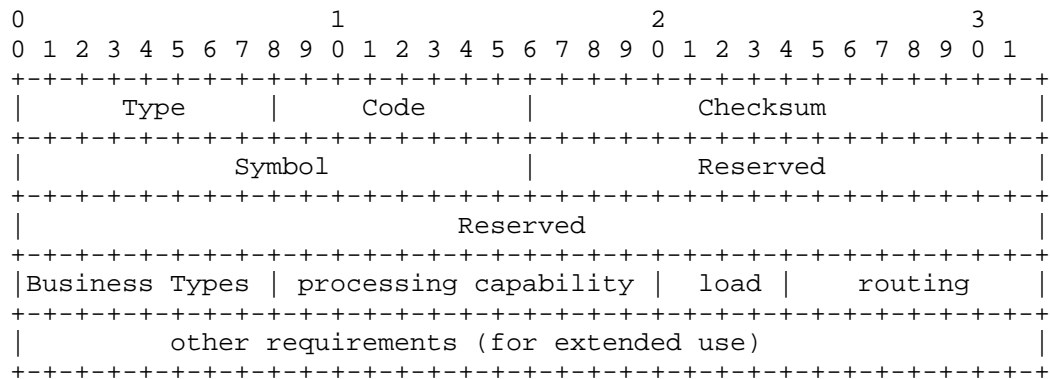


Figure 6 Specific Server DHP Query Message

o source address:IPv6 address of MN interface which send this message

- o destination address: DHP information management server address in CN domain
- o hop limit: 255
- o authentication header: if exists Security Association of IP authentication header between sending and receiving peer , the sending peer should include this header field
- o ICMP field:
  - type 164
  - code 0
  - checksum ICMP checksum.
  - retained this field is not used. The sender must initialize it to 0, the recipient must ignore it.
- o Options: the sending node must contain the following options in the request message sent:
  - MN business requirement description: include business type to be initiated, processing capability, load requirements and the routing request and so on, users can also make further needs customization expansion according to the actual situation.

#### 4.3.3.2.2. DHP Query Response Message

DHP query response message in this way is the same with the corresponding query response message in 4.3.2, the difference is that the message type code is 165 and the destination address is DHP management server address.

In particular, the CN can act as a DHP management server if it makes some upgrades and extensions. For example, the CN needs to be able to receive the DHP routing announcements of its domain and record the relevant information, while the normal CN doesn't have this feature.

#### 4.4. DHOA Request/Response Message

After choosing DHP, MN needs to apply a specific DHOA from the selected DHP, which is completed by sending a message of DHOA application. Based on the domain prefix information and address generation algorithm, DHP generate the corresponding DHOA address,



and then back the address information to the MN, message format is shown in Figure 7 and figure 8.

#### 4.4.1. DHOA Application Message

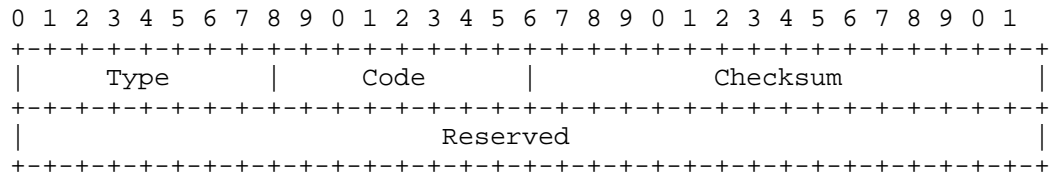


Figure 7 DHOA Request Message

- o source address: IPv6 address of MN interface which send this message
  - o destination address: DHP information management server address in CN domain
  - o hop limit: 255
  - o authentication header: if exists Security Association of IP authentication header between sending and receiving peer , the sending peer should include this header field
  - o ICMP field:
    - type 166
    - code 0
    - checksum ICMP checksum.
- retained this field is not used. The sender must initialize it to 0, the recipient must ignore it

## 4.4.2. DHOA Request Response Message

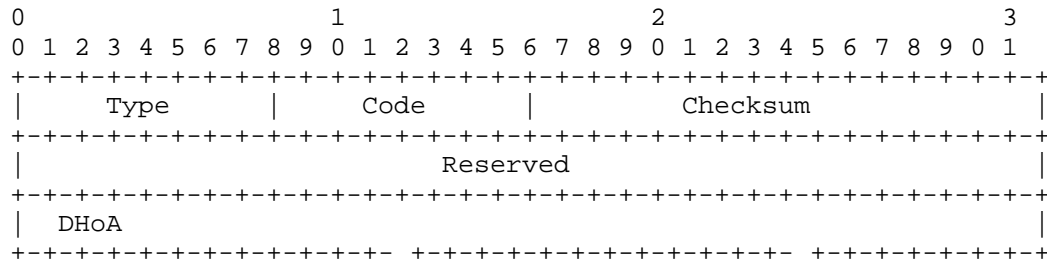


Figure 8 DHOA Request Response Message

- o source address: IPv6 address of MN interface which send this message
- o destination address: DHP information management server address in CN domain
- o hop limit: 255
- o authentication header: if exists Security Association of IP authentication header between sending and receiving peer , the sending peer should include this header field
- o ICMP field:
  - type 167
  - code 0
  - checksum ICMP checksum.
  - retained this field is not used. The sender must initialize it to 0, the recipient must ignore it
  - The transmitting node must contain the following options in the request message
  - DHOA address: distributed by DHP for MN

## 4.5. DHP Binding Update/Confirmation Message

In this standard, if the DHP service is enabled, then when MN moves, we need to judge whether to continue the current business, then make a DHP binding update for current CoA address. This binding update

message format is similar with the binding update message of BU in MIPv6, but needs extend a byte to store the corresponding business flow port number in its message extension headerto distinguish different traffic flows. The message format is shown in Figure 9. Binding update confirm message between DHP and MN is the same with BA in MIPv6. The message format can be seen in IETF RFC6275.

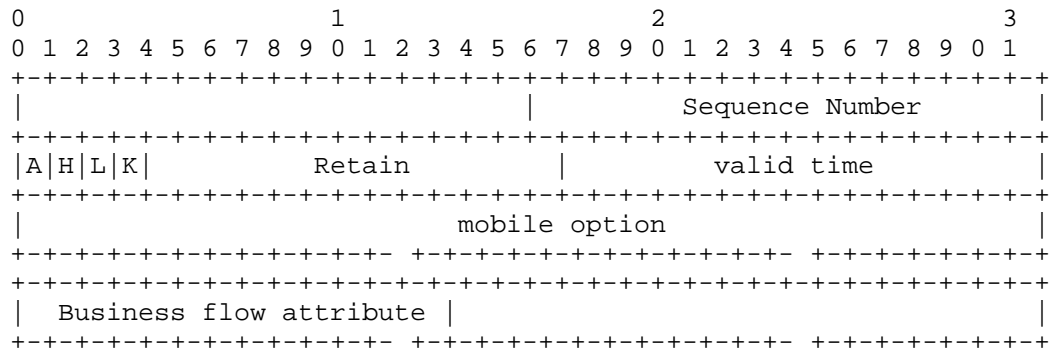


Figure 9 DHP Binding Update Message

- o sequence number: same with the BU message regulations of standard MIPv6
- o standard of related bits: same with the BU message regulations of standard MIPv6
- o valid time: same with the BU message regulations of standard MIPv6
- o retention
- o mobile options: same with the BU message regulations of standard MIPv6
- o extension field
- o The sending nodes contains the following options in the request message:
  - Business flow attribute, business port number when initiating business locally, used to identify a service flow between the host and the corresponding DHP.

## 5. DMIPv6 Workflow

This standard provides a distributed MIPv6 compatible solution named DMIPv6 which enables service flow distribution and handoff management. We assume that MN has already moved to foreign network from home network here, thus MN should have DHoA address and CoA address, or HoA address and CoA address if the DMIPv6 is unavailable. We introduce the main processing workflow of the technical proposal in this standard, with 2 steps: the processing procedure of the new service flows and the MN handoffs, which corresponds to the service flow distribution and mobility handoff management.

### 5.1. The Processing Workflow of New Service Connection

It is the processing workflow in the DMIPv6 when there is a new service connection between MN and CN. The detailed procedure is introduced as follows, and the related message interaction diagram is introduced in Figure 10. The detailed message format is shown in Chapter 4.

#### 5.1.1. The Decision of the Mobility Requirement of Service Flow

MN decides whether the service flow needs mobility support according to the service type of the new connection request. The standard of this decision can refer to the requirement of the MN itself and set the decision rule in advance:

If MN decides that the service flow needs mobility support, then it goes to section 5.1.2; or MN will use the old CoA address to establish the connection with CN.

#### 5.1.2. The Requirement Decision Started by the New Connection

Mobile nodes decide whether the new connection request is started by the local MN, if it is then MN goes to section 5.1.3; or MN uses HoA address to establish the connection with CN.

#### 5.1.3. DHP Query

MN queries the DHP address and status of CN's network for its service flow, and there are 4 ways to realize the DHP query, which can be found in section 4.3. Figure 10 provides the message interaction diagram for different ways of query. Figure 10(a) is for the query of dynamic discovery and multicast request in section 4.3.1 and 4.3.2. Figure 10(b) is for the query which introduces DHP management server or uses CN in section 4.3.3 and 4.3.4.

#### 5.1.4. DHP Selection

After the DHP query, MN needs to make the DHP selection. For the active query introduced in section 4.3, MN will decide which DHP serves itself according to different targets. The actual decision can be made in MN in advance, such as the distance to CN, processing ability, related workload information, etc. As for the passive query, MN can directly achieve the DHP address and the corresponding information.

Besides, during the process procedure of this standard, DHP always knows MN's location information and must ensure to avoid MN's information disclosure. As a result, the DHP selection introduces the selection of DHP's security mechanism. Each DHP will make its security warranty as one of the most important status information and can provide hierarchical classification on occasion. As for the active query in section 4.3, MN can decide to select which security level of DHP to serve it; as for the passive query, MN needs the related management server to make selection policy and directly achieve the related information. It is preferred that these security requirements are considered as an integral part of the DMM design.

#### 5.1.5. DHOA Address Application

MN will send the corresponding address application message to the DHP after deciding which DHP serves it. DHP can create the required DHOA message according to the address creation algorithm and local prefix information, and then inform the MN of this DHOA. At the same time, it will bind the allocated DHOA with MN's current address.

#### 5.1.6. Establishing the Communication Connection

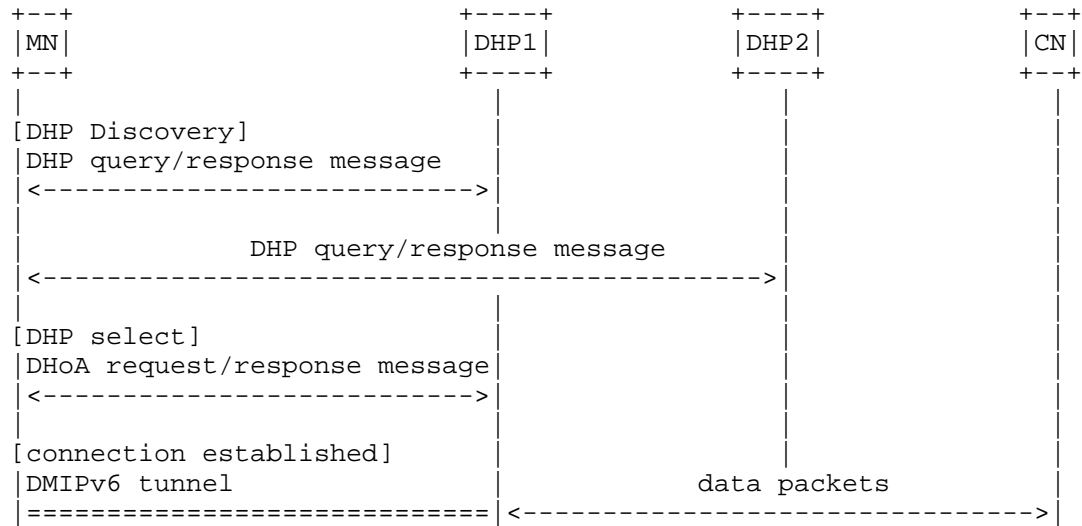
MN uses the queried DHOA to establish the connection with CN, and at the same time, DHP will save the information of DHOA and MN's address. It maintains a mapping table of the DHOA, MN and a service connection, and this mapping table is used for the management of mobility handoff.

A notice is that, MN will use HoA to establish the connection with CN if the DHP query is failed in DHP, which means no DHP is found to serve the current MN. Later workflow is the same as that defined in MIPv6.

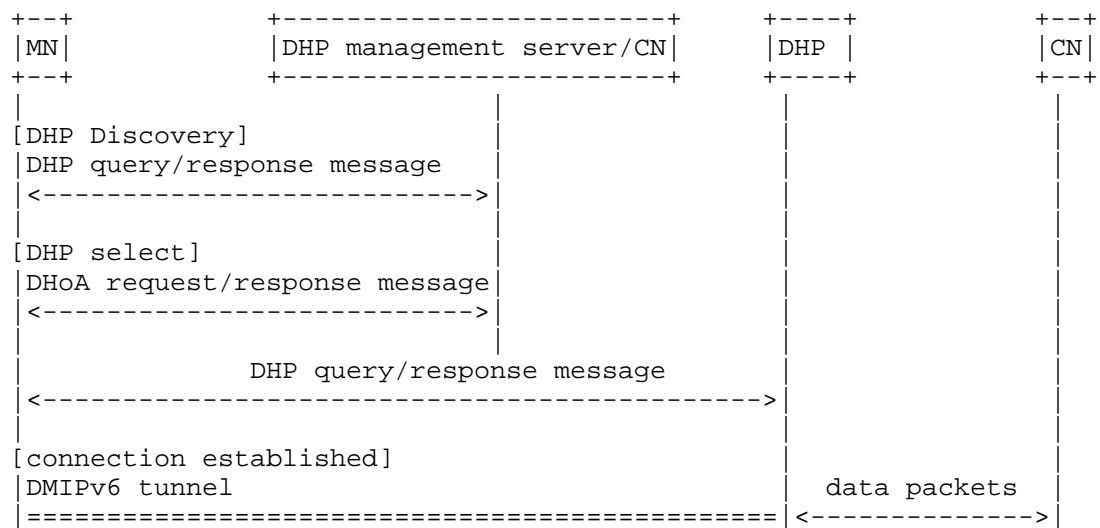
#### 5.1.7. Confirming the Communication Mode

MN needs to decide whether to use routing optimization mode or bi-direction tunneling mode according to the situation how CN supports the routing optimization. MN will use routing optimization mode for

the CN which supports routing optimization; or it will use the bi-direction tunneling mode. After confirming the communication mode, MN will start data transmission with CN.



(a)



(b)

Figure 10 New Service Connect Message interaction

## 5.2. The Processing Workflow when MN Moves

In the communication between MN and CN, when MN moves, first need to judge whether the DHP has been enabled. For the enabled DHP, to carry on the following steps, otherwise according to the standard MIPv6 protocol to execute.

### 5.2.1. The Qos Conditions Identification of A New Access Network

MN According to the Qos condition of a new access network, business priorities and the Qos requirement to judge whether the Qos requirement has been satisfied and whether the business should be continue. Specific we can achieve the condition of network interface, topology-aware, business flow parameter estimation of available bandwidth measurement, network packet loss rate and throughput to implement the requirement.

### 5.2.2. Handoff Management

For the service streams need to continue communication, will perform the following operations:

1. MN bind the CoA address and the port of the flow with the selected DHP.
2. DHP Replies binding update confirmation.
3. DHP performs proxy functions, intercepts the packets of CN sent to the MN existing home network, through the establishment of the tunnel DHP sent the packets to the new access network of MN.
4. For the CN of supporting the route optimization function, MN binds the new CoA address with CN, begin to communicate with CN until the CN's reply has been accepted. For the CN of not supporting the route optimization function, MN will carry on communication and transmission by bidirectional tunnel.

For the service streams that don't need to continue communication and Qos has no requirement. MN will stop the flow and will not bind the new CoA address with DHP.

For different businesses, MN can take different interrupt. Specifically, according to different transport layer protocols, and

its own characteristics MN will take different message exchange or notification.

## 6. Security Considerations

This standard is compatible with MIPv6, in the meantime, DHP equipments are added to it. Its basic procedures and messages exchanging schemes are similar to MIPv6, which lead to similar security issues like MIPv6's, including the security of dynamic DHP discovery, addresses binding and tunnels setting up between MN, HA, and CN. Detailed information in IETF RFC 6275.

This standard is compliant with standard MIPv6, which means MN still has HoA in home domain. When MN is initiating a new connection with DMIPv6, it will first apply for DHoA. According to MIPv6, MN's HoA is permanent during in its travelling, so CN always knows its HoA. So CN will see MN travel from home domain to network with same prefix like DHoA. In addition, DHP is commonly in CN's domain and is close to CN, so CN will identify that MN has already moved to place near itself. In the whole process, CoA is hidden from CN, which avoid some security risks to some extensions.

In the standard, DMIPv6 will be chosen when MN initates connection first. So, if there are random or periodic pseudo-connections, the process of DHP lookup and DHoA application will be triggered, which will impose heavy burden on MN and DHP. In fact, it's likely that from trojans and hackers' attacks. Under such circumstance, MN should use secured authentication to limit the number of pseudo-connections, and set bidirectional security mechanisms in DHP.

When DMIPv6 is turned on, DHP will always know MN's location, and can send the information to third parties, while those requests for location may be ill-intended. So, DHP needs to build enough security mechanisms to guard MN's information. Whether DHP has security mechanisms will be an important condition in MN's inquiry to DHP. Detailed information see 5.1.4.

## 7. IANA Considerations

This document proposes 4 DHP query methods, and 8 message types totally for them:

- o The Dynamic DHP Discovery Query Message, and the Dynamic DHP Discovery Acknowledgement Message, described in Section 4.3.1
- o The Multicast Request DHP Query Message, and the Multicast Request DHP Acknowledgement Message, described in Section 4.3.2



- o The Specific Server DHP Query Message, in Section 4.3.3.1.2
- o The DHOA Request Message, in Section 4.4.1
- o The DHOA Request Response Message, in Section 4.4.2
- o The DHP Binding Update Message, in Section 4.5

## 8. References

### 8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2460] Deering, S., "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, November 1997.
- [RFC4862] Thomson, S., Narten, T. and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.
- [RFC5944] Perkins, Ed., C., "IP Mobility Support for IPv4, Revised", RFC 5944, November 2010.
- [RFC6275] Perkins, Ed., C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

### 8.2. Informative References

- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5026] Giarretta, G. Kempf, J. and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, Oct 2007.
- [NTMS2008] Bertin, P., "A Distributed Dynamic Mobility Management Scheme designed for Flat IP Architectures.", NTMS'2008, November 2008.
- [I-D. yokota-dmm-scenario]

Yokota, H., Seite, P., Demaria, E., and Z. Cao, "Use case scenarios for Distributed Mobility Management", draft-yokota-dmm-scenario-00 (work in progress), October 2010.

#### Authors' Addresses

Min Liu

Institute of Computing Technology, Chinese Academy of Sciences,  
No.6 Kexueyuan South Avenue, Zhongguancun, Beijing 100190, China  
Email: liumin@ict.ac.cn

Yuwei Wang

Institute of Computing Technology, Chinese Academy of Sciences,  
No.6 Kexueyuan South Avenue, Zhongguancun, Beijing 100190, China  
Email: wangyuwei@ict.ac.cn

